

Nigeria - [419 Coalition](#) 2012 News on Nigerian Scam / 419 Operations

19 NOV 2012

From the Nigerian newspaper The Guardian:

In London, Nigerian gospel artiste jailed for defrauding online lovers of 120,000 UK Pounds

From Tunde Oyedoyin, London News - Metro

A NIGERIAN gospel singer, Oluwamayowa Ajayi, who fleeced four American women he met on the internet dating site, Match.com, of over £120,000 was jailed for six and a half years on Friday evening at Snakesbrook Crown Court in East London.

Ajayi, 31, who is an overstayer in Britain, looked blank and showed no outward emotions as he was handed the sentence. As if resigned to fate, he walked sheepishly behind one of the two female security guards who led him out of Courtroom 20, where his fate was sealed.

About a minute earlier, Judge Sarah Paneth told him, "I'm sentencing you to six and a half years. You may now go down - a technical term for jail."

Ajayi, who performs under the stage name, "Malo Joe" pretended to be an American fighter pilot, a grieving widower and an oil executive to the women he fleeced before the long arms of the law caught up with him.

Prior to his sentencing that evening, both the crown prosecutor and his defence counsel spent close to two hours making last minute submissions to the Judge.

While the crown prosecutor summed up his argument stating how Ajayi lived off the women by lying -among others, in one instance - that he had been held hostage by Niger Delta militants and therefore, his captors needed some ransom before he could be released, otherwise, they would kill him, his defence lawyer, John Femi-Ola pleaded with the court: "Don't crush him so that he can have the opportunity to do something useful with his life," after his term. Femi-Ola also told the Judge that "this is his first time."

Despite the pleas for mercy, it was inevitable that he would be caged. After listening to the pleas from both sides, the Judge took a 20- minute break at 3.40p.m. and when the court re-convened at 4.00p.m., she took about 40 minutes to read her sentencing notes, detailing the seven- count charge that Ajayi had been found guilty off by the jury who had found him guilty four days earlier.

In one instance, she tricked and lied to one of his victims who parted with over \$100, 000, that he was a businessman who was short of cash and therefore, needed a loan. The woman used some of the money on her credit card and also borrowed from family members to raise the funds.

In another, Ajayi claimed he was in the hands of Niger Delta militants and they would kill him within 20 hours if the woman didn't do anything about the ransom they asked her to pay. She hurriedly sent \$500 through Moneygram to Nigeria, where he then cashed the money.

According to the Judge, "all the four women were embarrassed" when each discovered they were dealing with a con man and not someone who loved them and was in a relationship. Of course, none knew about the other until detectives contacted them after his arrest.

The Judge told him, "you defrauded women of the sums the women cannot afford to lose."

Ajayi, the Judge noted, would have continued preying on more innocent women had the arms of the law not caught up with him. As the Judge read her notes, his well wishers, numbering about seven, gasped and he looked resigned to his imminent fate before the curtains fell on his fraudulent life at 4.40p.m., when the judge told him, "I'm sentencing you to six and a half years. You may now go down." The court guards wasted no time in sandwiching him between themselves as they led him out of the courtroom.

Although it's not certain if he will be deported after his term, but Ajayi, who initially came to the United Kingdom (UK) on a six month visa in 2004, overstayed. He then left and on his return to the UK, falsely obtained a driver's licence using the name of a Portuguese man who had died in 2004. This, the Judge noted, showed that the gospel singer was a chief in the criminal operation for which he was being jailed.

Here is the URL of the article for as long as it is good:

http://www.ngrguardiannews.com/index.php?option=com_content&view=article&id=105244:in-london-nigerian-gospel-artiste-jailed-for-defrauding-online-lovers-of-419-scams

31 OCT 2012

From the Toronto Star online site, the star.com:

Will Ferguson takes Giller Prize for novel 419

by Greg Quill

Tuesday night at the Ritz-Carlton hotel. Calgary-based humourist Will Ferguson's 419, a bleak mystery centred on the dark world of Nigerian Internet scams, was on Tuesday night named winner of the 2012 Scotiabank Giller Prize, the nation's most prestigious literary award - and with a \$50,000 purse, the most valuable.

"I'd like to thank my long-suffering editor and Penguin Canada for supporting my possibly ill-advised shift to fiction," said Ferguson, 48, who attended the Giller Prize gala at Toronto's Ritz-Carlton Hotel in full highland regalia, including kilt, dirk and sporran.

The crowd favourite and a confident showman, Ferguson also thanked his Japanese wife, Terumi, his mother and siblings for their support, and Toronto doctor-turned-novelist Vincent Lam, a previous Giller winner, "for endorsing a very unlikely book."

Standing on the Ritz-Carlton ballroom stage in front of 500 writers, publishers, politicians and arts supporters in all their finery and a full CBC-TV crew that was recording the proceedings for later broadcast Tuesday night, Ferguson dug into his sporran and withdrew a flask, then invited the crowd to "raise a toast for the written word."

Ferguson, a three-time Leacock Medal winner for humour and a successful writer of travel memoirs, said after the presentation that he had not started out to write a dark novel.

"It began with the thought that maybe there really is a Nigerian prince somewhere who can't gain his freedom for lack of funds . . . but when I started writing it, the story began to turn dark, all by itself."

Amid the flash and glamour drummed up with increasing ferocity by the CBC and Giller founder, businessman/philanthropist Jack Rabinovitch, Ferguson seemed perfectly at home.

"Look, I love that in Canada literature gets the red carpet treatment," he grinned.

His next book will not follow the sombre fiction trail, he added.

"It's a travel book about Rwanda. I try to switch between fiction and travel because each discipline uses different parts of the brain."

Ferguson's book was selected over Alix Ohlin's sophomore novel, *Inside*, an exploration of the hidden dangers in human relationships; Nancy Richler's *The Imposter Bride*, about a woman's search for the mother who may or may not have abandoned her; Kim Thuy's 2011 French-language Governor General's Literary Award-winning memoir, *Ru*; and Russell Wangersky's collection of death-dealing short stories, *Whirl Away*.

This year's Giller jury comprised American satirist Gary Shteyngart, Irish author Roddy Doyle and Canadian publisher and writer Anna Porter. This is the Giller's 19th year.

The jury read 142 works of fiction, submitted by 50 publishers from every region of the country.

Of all Canadian literary prizes, the Giller has emerged as the most glamorous and rewarding, thanks largely to Rabinovitch's acumen and a deal he inked two years ago with CBC, turning an otherwise staid literary event into a major cross-promoting TV spectacle, complete with variety trappings.

On the bill this year as presenters of the five nominees were political satirist and CBC-TV comedian Rick Mercer, Golden Globe-winning actress Kim Cattrall, Juno-winning Canadian soprano Measha Brueggergosman, TV writer, producer and actor Allan Hawco, Olympic gold medal gymnast Rosie MacLennan, as well as CBC radio host Jian Ghomeshi, the night's MC.

Entertainment was provided by Jacob Hoggard, from the award-winning B.C. band Hedley, who was accompanied by a dance sequence choreographed by Jorden Morris, former principal dancer with the Royal Winnipeg Ballet.

Here is the URL of the article for as long as it is good:

<http://www.thestar.com/entertainment/books/article/1280103--will-ferguson-takes-giller-prize-for-novel-419>

419 Coalition Note: We congratulate Mr. Ferguson on his novel and the recognition he has received for it. Education remains one of the best ways to deal with 419, and the more folks who read "419" the better! However, it is important to note that while "419" is an excellent read, it is purely Fiction. For those interested in further reading on 419, there are additional works available on the subject, like Brian Wizard's "[Nigerian 419 Scam : 'Game Over'!](#)" and others listed in the "Books and Movies on 419" section of our main page.

12 OCT 2012

From the Nigerian Tribune newspaper, via Odili.net, which, along with Nigeriaworld, are excellent sources of news and information on Nigeria. Both are operated by Mr. Chuck Odili, a highly educated top of the line Nigerian professional, entrepreneur, and IT expert, who deserves kudos for his sustained effort on these and other Nigeria centric sites over these many years:

\$9,200 online scam: Undergraduate bags 18-year jail

Written by Yejide Gbenga-Ogundare

Justice Aishat Opesanwo of a Lagos State high court sitting in Ikeja, on Thursday, sentenced a young man, Michael Opaleye, to 18 months imprisonment for perpetrating a \$9,200 Internet scam.

Opaleye, who claimed to be a student of the University of Lagos, was tried and convicted for defrauding an American lady, Kathy Lunsford, of \$9,200 on the pretext that he would marry her.

When he was arraigned, Opaleye, who said he is a Computer Science undergraduate at the University of Lagos (UNILAG), had pleaded guilty to the charge of obtaining money

by pretence and forgery.

He had entered into a plea bargain with the Economic and Financial Crimes Commission (EFCC) and offered to pay the money to his victim.

Justice Opanwo, while delivering judgment, said the sentence would take effect from March 15, 2012, when he was first arraigned before the court.

She also ordered Opaleye, after his jail term, to pay N100,000 monthly to the victim through the EFCC until he refunds the total amount involved in the scam.

The convict is also to forfeit the electronic appliances and other items purchased with the proceeds of the crime, which were recovered from his house during the investigation, to the anti-graft agency.

Counsel for EFCC, Mr Anselem Betram Ozioko, said Opaleye had, between 2008 and 2011, swindled Lunsford by making a phoney marriage proposal to her through e-mail communications.

According to him, Lunsford had sent Opaleye the said amount as part of his travelling expenses from the United Kingdom to the United States of America to facilitate their wedding.

Ozioko said the defendant forged a driver licence, which he claimed was issued by the Federal Road Safety Corps (FRSC) and a bank draft, which he claimed was issued by the Bank of Ireland, Dublin.

The offences, according to him, contravened and were punishable under Sections 419 and 467 of the Criminal Code Laws of Lagos State 2003.

Here is the URL of the article for as long as it is good:
<http://odili.net/news/source/2012/oct/12/615.html>

419 Coalition Note: We commend the EFCC and the Court for their work in this case; particularly for the Court Ordered Restitution to the victim with EFCC supervision and monitoring of same.

18 JUL 2012
From the Sydney Morning Herald, Australia, sent in by
Ultrascan AGI:

From Nigeria with love

Nigerian scammers are back with a vengeance, more sophisticated than before and using online dating and auction sites to rip off tens of millions of dollars a year from vulnerable Australians.

by Eileen Ormsby

Even our computer recognises when something is too good to be true, so we don't see them so much any more - those emails offering untold wealth if we help a dignitary move a fortune from a hostile country, or notifying us of massive winnings in lotteries we don't recall entering. And for the few that don't go straight to junk mail we hit "delete" without another thought.

Why, then, are tens of thousands of Australians still losing more than \$55 million a year to mass-marketed advance fee fraud (scams tricking people into paying money upfront to secure a financial or emotional benefit at a later date), more commonly known as "Nigerian" or "419" scams?

Some may think it could never happen to us because we, and our computers, have become more sophisticated. But, then, so have the conmen.

"Scammers are constantly evolving and finding new ways to trick victims into parting with their money," says Ken Gamble, of Internet Fraud Watchdog.

The scammers who used to send us the emails are now finding their victims through legitimate dating and auction sites. In what have become known as romance scams, once the fraudsters hook their victim they use voice-changing devices to hide Nigerian accents or employ sophisticated software to make victims believe they are video chatting with attractive models.

Last year, consumer watchdog the Australian Competition and Consumer Commission received reports that put money lost to romance scams at more than \$22 million, with an average loss of \$21,000 per victim.

In romance scams, victims meet fraudsters through online dating sites and part with money to buy airfares, secure early discharge from the army or help a sick relative of a person the victim believes is in love with them.

The \$5000 that Meredith Hoarey lost was all the money she had saved. She believed the man she had met online was an American soldier based in Iraq. In telephone and internet conversations over nine months, "Sgt Zachary Smertyn" convinced Hoarey, 46, of his intention to be discharged from the US Army so that he could come to Australia to marry her.

His alleged commander told her via webcam that Smertyn could not be discharged until certain expenses had been covered. He sent her a variety of official-looking documents to "prove" his claims, as well as a "Military Wife Registration Form".

Believing it was the only way she could be with the man she had fallen in love with, Hoarey, who lives in NSW, sold her car to cover the expenses. Soon after, she received a bill for \$3000 for a weapon allegedly lost by Smertyn, which she was told had to be repaid before he could be discharged.

"That's when my whole world came crumbling down - I knew I'd been had," she says. "I felt like part of me had died. How could I be so dumb?"

Miriam Munro* knows this feeling only too well. She sent \$60,000 to a man she believed to be an American businessman called "Dayne", whom she had met on a well-known internet dating site.

She had heard of Nigerian scams, but she had no reason to believe she was being subjected to one because Dayne told her he lived just an hour away from her home in Western Australia. He even gave her a local phone number to contact him on, but then said he couldn't meet her because he was travelling on business. In reality, the "local" number diverted to Nigeria.

In retrospect, he fell for Munro very quickly. "They love bomb you. They send emails, they send love poems, they talk to you on Messenger, they ring you two or three times a day," she says.

It is easy to dismiss victims of 419 scams as stupid or gullible, but Munro comes across as neither of these; she is in her 50s, is articulate and holds down a professional job. What she was, she readily admits, is "lonely and vulnerable and going through some personal strife".

Gone are the days of emails full of laughably broken English and absurd claims of outrageous rewards for very little effort on the part of the victim.

"I was totally convinced I was talking to an American girl and an American guy," Munro says. Her conviction was not unreasonable, given she spoke to him on the phone and communicated with both him and his "daughter" over a webcam. "I would talk to them all the time."

But the voices and webcam videos were fakes and it turned out all communication was coming from Nigeria, still a hub for online fraudsters. Increasingly sophisticated in the running of the scams, they work in shifts and use voice changers to give themselves an American accent.

Sophisticated programs, such as that offered by CamDecoy, provide videos of models that can be manipulated by the scammers to appear as though they are interacting with the victim on a webcam. Even more sinisterly, fraudsters use footage of unsuspecting members of webcam chat rooms that has been recorded surreptitiously over several weeks.

In both cases, the scammers claim there is a problem with sound but have full control over the footage. They can pause it, type when the person on screen is typing, or jump to a clip of the model waving, laughing or otherwise reacting as the victim would expect them to.

For example, Dayne bombarded Munro with flowers, cards, telephone calls and webcam chats. "He said everything I wanted to hear, I needed to hear," she says.

After a few months, the requests for money began. First he needed a loan when he became stranded in Ireland. Then he offered to invest some of Munro's funds into his successful business. Believing his professions of love and that he yearned to hurry back to Australia to be with her, she handed over \$60,000.

Finally, unwilling to wait any longer, Munro decided to go to Dubai to meet him. The night before she was due to leave, he phoned her. "He said his daughter had been in an accident and he couldn't meet me at Dubai airport. And then, I just knew."

She was devastated. Not only had she lost money, she had also lost what she thought was the love of her life - and her ability to trust people.

Donald Thomson, a forensic psychologist at Deakin University, says the impact on the interpersonal relationships of victims who commit themselves emotionally as well as financially is greater than those who are victims of a purely financial scam. "They can separate themselves from it, but the person who has been a victim of a romantic scam has given all of themselves."

Meanwhile, "The Psychology of Scams", a study commissioned by the UK Office of Fair Trading, shows people who have already been a victim of a scam are consistently more likely to show renewed interest in contact from fraudsters. One trick of conmen is the "secondary scam" in which they contact a victim some time after they realise they have been scammed and pretend to be lawyers, government officials or police from the scammer's country.

This happened to Munro. "Sean King", whom she chatted with on another site, told her he had also been the victim of a scammer. He said the Economic and Financial Crimes Commission, a Nigerian law enforcement agency that investigates 419 scams, had helped him and a friend to recover their money. Her local police had already suggested she get in touch with the EFCC, but "I emailed them and never got a reply," she says. Sean told her he would get the employee who had helped him to contact her. "So he [the EFCC employee] emailed me and then it was all on again," Munro says.

The emails had the same EFCC logo as she had seen on the site to which the Australian police had directed her. "They said because such a large amount of money was due to me, I had to get anti-money-laundering and insurance certificates from the bank. All the documents

that came to me looked totally believable," she says. "They named the guy who scammed me and said they had his IP address. It was very clever. I was sucked in."

Thousands of dollars later for a variety of "fees" and "certificates", Munro realised she was being scammed again.

While romance scams target the lonely and vulnerable, usually people over 50, another type of scam targets the young and naive. The ACCC research showed an increase in "high volume scams" that catch more victims, but for smaller amounts of money.

Brittany Smith, who lives in Melbourne, was just 17 years old when she lost her life's savings trying to buy a car from a well-known Australian car sales website. When she found one she liked, the seller told her that the site would hold payment in escrow until she confirmed she was happy with the car. Smith soon received an email on the site's letterhead.

"It looked legitimate," she says of the email, which contained both hers and the seller's information. "It had contact details for a site representative and said I had to give it \$7000, which they would hold on to until the car was delivered and I told them to release it."

Four days later, she still hadn't heard from the seller and was unable to contact the "representative". So Smith called the website to get her money back and that's when she learnt she had been scammed. "They told me they have no communication whatever with buyers or owners; all they do is run the site."

Like most scams, payment was made through Western Union. Smith knows now that Western Union should never be used to transfer money to people unknown. "In hindsight, when you look at it, you think, yeah, there were some alarm bells but at the time it seemed so legitimate."

She contacted the Australian Federal Police but was told there was little it could do. The ability of scammers to operate in a variety of countries means that few offenders are arrested and prosecuted.

A representative of NSW Police who is responsible for Meredith Hoarey's case says on a cost/benefit analysis it was not worthwhile tracking the culprit to Nigeria and there was no "reasonable prospect of conviction", which is necessary for a prosecution to proceed.

An AFP spokesperson says it has no legal right to make inquiries or conduct an investigation in a foreign country. "However, the AFP works closely with international law enforcement, including Nigerian authorities, Australian law enforcement and industry to combat online crime of this nature in a holistic fashion."

The consensus among these agencies and others is that a victim of an online scam is unlikely to recover any of their money.

The Australian Institute of Criminology says "the best approach lies with prevention, in raising awareness and in encouraging potential victims not to respond to invitations in the first place". A spokesperson says: "Our role is education and awareness, but we do work with a number of agencies, both Australian and overseas, to try and disrupt scammers."

On Valentine's Day this year, the ACCC released voluntary "Best Practice Guidelines for Dating Websites", which most major dating sites claim to abide by. Some sites will not allow registrations from outside Australia, but Peter Brittain of Slinky.com.au says scammers work with Australian associates. Indeed, scammers use agents in Australia partly to stop alarm bells going off when victims are told to send money to Nigeria. Hoarey, for example, transferred money through Western Union to recipients in Queensland.

Earlier this year, Brisbane woman Sarah Jane Cochrane-Ramsey, 23, was convicted of fraud after being employed by Nigerian scammers to provide an Australian bank account through which they could funnel payments they received through a popular car sales website. Her payment was to be 8 per cent of all money received, but instead she kept the \$33,000 she received, fleecing both victims and scammers.

Ken Gamble's company, Internet Fraud Watchdog, tracks IPs of fraudsters for those who can afford his services. He warns of an increase in investment scams, such as boiler-room fraud (cold calls offering investors worthless, overpriced or non-existent shares) and online sports betting fraud, backed by slick websites, glossy literature and fast-talking salesmen.

The Office of Fair Trading study shows that, surprisingly, it is people who are educated in the stockmarket and gambling who are most likely to fall for these scams and fraudsters, particularly retirees looking for better returns on their superannuation.

For Brittany Smith, being scammed was a wake-up call. "Being 17 years old and losing every cent I'd worked for was horrible. I was just shocked that people even did that. It was a bit of a reality check. I'm in the real world now and people do this kind of stuff."

* Miriam Munro is not her real name. It has been changed to protect her identity.

Eileen Ormsby is a Melbourne journalist. She blogs at allthingsvice.wordpress.com

Here is the URL of the article for as long as it is good:

<http://www.smh.com.au/digital-life/consumer-security/from-nigeria-with-love-20120717-228bi.html>

17 JUL 2012

From PSNEWS Australia, sent in by Ultrascan AGI:

AUSTRAC cashes in on money laundering

A new report by the financial intelligence unit, AUSTRAC, shows how money laundering and other offences pose a threat to Australian businesses and the community.

Launched by the Minister for Home Affairs and Justice, Jason Clare, the AUSTRAC typologies and case studies report 2012 includes 21 real-life case studies featuring an array of offences including large-scale tax evasion, advance fee fraud and investment scams, identity theft and drug trafficking.

Mr Clare said the case studies showed Australia's strong economy was making the country a tempting target for transnational and high-tech crime.

"It also confirms that when government and industry work together we can catch the criminals responsible," Mr Clare said.

"AUSTRAC analyses financial information and shares this information with a range of government law enforcement and other agencies, which has led to asset seizures and the arrest and conviction of criminals."

He said case studies from the 2012 report showed how AUSTRAC and its partners uncovered a range of serious offences including manufacturing businesses using shell companies, cheques and secret cash payments to undertake large-scale tax evasion.

He said an extensive Nigerian 'advance fee' fraud had been uncovered in which more than 20 Australian victims lost millions of dollars[emphasis by 419 Coalition], as had a criminal syndicate which stole the identities of victims to perpetrate a multi-million dollar superannuation fraud.

"The report analyses two established money laundering methods - the use of cheques to launder money and evade tax and the use of third parties to carry cash across borders - as well as a number of emerging money laundering vulnerabilities," Mr Clare said.

"Authorities and Australian businesses should be alert to the potential threats posed by new payment systems, including digital currencies and virtual worlds, voucher system products and offshore online money remitters."

"This report examines these risks, and lists a number of ways to help business and the wider community identify the possible misuse of these emerging systems."

Here is the URL of the article for as long as it is good:

http://www.psnnews.com.au/Page_psn32212.html

9 JUL 2012

From the Punch, a Nigerian newspaper:

Woman arrested for N28m fraud

by Eniola Akinkuotu

The Police Special Fraud Unit, Lagos, have arrested a 33-year-old woman, Bunmi Akintoye, for allegedly defrauding various people of over N28m.

In a statement by the Head, Public Affairs, SFU, Mr. Pius Afachung, the police said the suspect was being investigated due to sundry allegations levelled against her by different persons.

Afachung said, "In one of the cases, Akintoye obtained 96 pieces of Hewlett Packard Laptops in June, 2011 from one of her victims at the cost of N105, 000 each which amounted to a total sum of N10.08m. Akintoye criminally confused her victim into believing that she was a genuine business woman by depositing N1.5m and issuing post-dated Skye Bank cheques in the value of N8.5m which all bounced on presentation."

"In another case, the suspect approached one man in Ibadan, Oyo State, claiming that she won a contract from Lead City University in Ibadan. She obtained a total sum of N6m from the unsuspecting victim."

"In yet another case, this suspect obtained \$80,000 (N12.8m) from a United States-based Nigerian lady on the pretext of carrying out a legitimate transaction. In each of these cases, the suspect will vanish into the thin air, so to say, and would no longer pick calls from her victims."

Afachung added that investigations were ongoing and that the suspect would be charged to court soon.

The Commissioner of Police, SFU, Tunde Ogunsakin, seized the opportunity to warn members of the public to investigate business proposals before investing, to avoid falling victim to fraudsters.

Here is the URL of the article for as long as it is good:

<http://www.punchng.com/metro/woman-arrested-for-n28m-fraud/>

21 JUN 2012

From online magazine Slate.com:

The Other Reason Spammers Claim They're Nigerian: They Are Nigerian

By Will Oremus

In the Slatest, Jeffrey Bloomer has an interesting post on why email scammers claim to be from Nigeria, a country that has become almost synonymous with email scams. A new paper from Microsoft Research's Cormac Herley offers an ingenious explanation for the implausibility of the famous hoax: The scammers want most people to know it's a scam. With limited time and resources, they only want the most gullible people to respond. So "Nigeria" functions as a sort of code to weed out responses from people who wouldn't be likely to actually hand over any cash.

It's a hypothesis I've heard before, but I've never seen the case made nearly as convincingly as Herley makes it. For those interested, the paper itself is well worth a read. I have just two things to add.

One is that, as thorough as Herley's paper is, it doesn't purport to prove that scammers deliberately make their emails implausible. He didn't actually ask any scammers why they claim to be Nigerian. His theory is backed up by math and logic, not empirical evidence. What the paper shows is that bogus-sounding emails filled with cliches would make an effective strategy for weeding out false positives.

The second point is so simple that most readers might have already assumed it, but it was never explicitly addressed in the paper or much of the media coverage. The other reason that so many email scammers claim to be from Nigeria is that they are in fact from Nigeria. For a combination of reasons, Lagos has long been the world capital of advance fee fraud scams. In fact, the Nigerian email scam has been around since before most people used email - fraudsters in Lagos sent similar appeals via snail mail in the 1980s. The scams are often called 419 fraud, apparently in reference to the section of the Nigerian criminal code that covers such scams.

It's impossible to get precise figures on where email scams originate, but experts estimate that well over 50 percent of advance fee fraud emails come from Nigeria. The Dutch firm Ultrascan Advanced Global Investigations used to publish an annual report on 419 scams. In the latest report I could find, from 2009, they counted at least 250,000 that originated in Nigeria, with another 50,000 or so coming from 69 other countries around the world.

Other countries have, for various reasons of their own, become hubs for other types of cybercrime. Hackers who steal customers' credit card information from restaurants often hail from Russia. The FBI last fall traced one of the world's largest click-fraud scams to a ring of cybercriminals in Estonia.

So Herley's paper explains why Nigerian email scammers admit to being from Nigeria. Why Nigerians become email scammers in the first place is, perhaps, a question for another paper. My guess is that it's some combination of tradition - once a few Nigerians started making money this way, others followed - access to technology, high unemployment, and relatively weak law enforcement.

Security experts tell me the Nigerian government has been stepping up its efforts to go after scammers, but Lagos is one of the world's most crowded and fastest-growing cities, and prosecuting cybercrime is difficult even in the best of circumstances. It's not impossible, though: In 2009, U.S. authorities tracked down and convicted a Nigerian cybercrook who had immigrated to the United States the previous year. The rare prosecution showed just how lucrative the scam can be: Over a six-year period, the man had bilked 67 victims out of \$1.3 million.

Here is the URL of this article for as long as it is good:

http://www.slate.com/blogs/future_tense/2012/06/21/nigerian_email_scam_spammers_really_are_from_nigeria.html

Here is the URL of Mr. Herley's paper from Microsoft Research:

<http://research.microsoft.com/pubs/167719/WhyFromNigeria.pdf>

419 Coalition note: In the article above, the most important line for our readers to note is this:

"The other reason that so many email scammers claim to be from Nigeria is that they are in fact from Nigeria"

Also, 419 Coalition would like to add that we, as well as most counter-419er NGO's and governmental agencies we know of, are well aware that Nigeria 419er syndicates tend to open "branch offices" abroad at their earliest opportunity. One of the reasons they do this is to Disguise the origin of their 419 solicitations by removing Nigerian identifiers from them.

That being the case, even though Mr. Herley's math may be impeccable, in reality the 419ers are generally trying to do exactly the opposite of their "best course of action" as outlined for them in his study. It is the 419 Coalition's view that things are really much simpler than the study would indicate.

Our view is that many 419er cells continue to use Nigerian identifiers simply because they Are in Nigeria and haven't been able to figure out a way to disguise their actual location as yet.

Our experience is that 419ers see Nigerian identifiers as a Hindrance to their operations rather than as an asset in terms of victim targeting. What we see as the trend in 419 has been for many years that the 419ers try to Avoid using Nigerian identifiers in their solicitations whenever they can, and also to operate "branch offices" from countries other than Nigeria whenever they can, in part to further that strategy.

Therefore, Mr. Herley's math may be excellent, but in terms of 419 operations in the real world, the math simply is not applicable to 419 matters. We and other counter-419 NGO's have written to Mr. Herley strongly expressing our views to that effect in this matter.

The bottom line is that, real world, Mr. Herley's paper does NOT in fact explain why so many 419ers use Nigerian identifiers. 419ers simply do not operate the way they do for the reasons he says they do. The facts simply do not fit his hypothesis. It's too bad they don't. Counter-419 operations would be much easier if they did.

19 JUN 2012

From The Denver Post, sent in by a concerned Nigerian:

Brighton mom-daughter team accused of \$1 million online dating scam

A Brighton mother-daughter team stands accused of helping steal more than \$1 million from hundreds of women in an elaborate, multinational online dating scam, according to an indictment announced Tuesday by Colorado Attorney General John Suthers.

Tracy Vasseur, 40, and her mother, Karen Vasseur, 73, face felony charges of racketeering, money laundering, forgery and theft. The elder Vasseur could face up to 172 years in prison if convicted. Her daughter could face up to 205 years.

For three years, the pair allegedly collected money from 374 women in more than 40 countries for unknown Nigerian bosses.

The scam allegedly worked like this:

Unknown agents would pose as male soldiers stationed in Afghanistan and strike up online romances through online dating sites, e-mail and social networks.

As time passed and the relationships progressed, these "soldiers" would ask for money purportedly to buy a satellite phone so the "couple" could talk or to pay for a visit to the unsuspecting paramour. The scammers sent photos and forged military documents to bolster their cases, according to authorities.

Some women gave tens of thousands of dollars, including an alleged victim in Great Britain who wired a fake soldier nearly \$60,000.

That money was wired to Colorado, where the Vasseurs allegedly collected it, took their 10 percent and wired the remainder back to Nigeria, according to a Colorado state Grand Jury indictment handed down today.

Authorities believe the Vasseurs - who didn't solicit money from the alleged victims themselves - laundered their share through 20 personal accounts at local banks. The mother and daughter continued the activity even after being warned in 2011 by Brighton police, according to the indictment.

Tracy Vasseur bonded out of Adams County Jail on Monday. Karen Vasseur, remains in custody. The pair will be prosecuted in Adams County District Court.

Jessica Fender: 303-954-1244 or jfender@denverpost.com

Here is the URL the article for as long as it is good:

http://www.denverpost.com/breakingnews/ci_20892031/brighton-mom-daughter-team-accused-1-million-online

[*Read* the indictment against Tracy and Karen Vasseur \(PDF, 27 pages\)](#)

for as long as the URL is good

1 JUN 2012

From BBC News:

Benin: US 'internet scam victim' freed by police

A US national kidnapped last week in Benin has been freed by security forces and two of his Nigerian abductors arrested, an official has said.

The man, who has not been identified, is believed to have travelled to the West African nation after reportedly being targeted by cybercriminals.

His kidnappers forced him to contact his family for a ransom, police said.

In recent years, there have been a number of foreigners held for ransom in West Africa after internet scams.

Correspondents say they often fall victim to promises of lucrative business opportunities.

Such kidnappings are rare in Benin, but there have been several cases in neighbouring Nigeria.

Pierre Dovonou, an expert on cybercrime based in Benin, told the BBC's Network Africa programme that, as a result of a Nigerian police crackdown on internet fraudsters, many had crossed over the border and were working from the former French colony.

"The kidnapped American has just been found in [the south-west] Mono region and two of his kidnappers, Nigerians, were arrested and are in the hands of the police in Benin," a spokesperson for Benin's interior ministry, Franck Kinninvo, told the AFP news agency.

"He was found with the combined efforts of the FBI and Benin police," Mr Kinninvo said.

The details of the case are unclear, a spokesperson for the US embassy in Nigeria said,

AFP reports.

Security sources told Reuters news agency that the man had travelled to Benin to meet up with a group of people from that country and neighbouring Nigeria that he had met on the internet.

Here is the URL of the article for as long as it is good:
<http://www.bbc.co.uk/news/world-africa-18293883>

The story was also covered by Globalpost.com, here is the URL as long as it is good:
<http://www.globalpost.com/dispatch/news/regions/africa/120602/us-national-kidnapped-benin-after-internet-scam-freed-police>

30 MAY 2012

From the Nigerian newspaper, Vanguard:

American kidnapped in Benin victim of Internet scam

COTONOU (AFP) An American abducted in the West African nation of Benin is believed to have fallen victim to an Internet scam and a ransom has been demanded for their release, a police source said Wednesday.

"It is a case of cybercrime and the victim was trapped," a police source in Benin said on condition of anonymity because of the sensitivity of the matter.

"The criminals are in contact with the family in the United States and they are demanding a ransom."

Details of the kidnapping remained unclear. A US embassy spokeswoman in neighbouring Nigeria at the weekend said a US citizen had been kidnapped in Benin last week, but could provide no further details.

A message on the US embassy in Cotonou's website on Wednesday said "a US citizen was recently kidnapped in Benin. The US embassy in Cotonou has no reason to believe that other US citizens or interests are at risk."

It said no other details were being provided for now and added that an investigation was ongoing.

Security sources in Benin say the victim was thought to have crossed into the country on May 22 from Togo, where he met up with a group that included Nigerians.

Kidnappings have been rare in Benin, a former French colony of some nine million people, though they occur regularly in Nigeria, Africa's most populous nation and largest oil producer.

A number of people have been kidnapped for ransom in Nigeria after having fallen victim to Internet scams promising lucrative business opportunities.

Here is the URL of the article for as long as it is good:
<http://www.vanguardngr.com/2012/05/american-kidnapped-in-benin-victim-of-internet-scam/>

17 APR 2012

From the Punch, a Nigerian newspaper:

EFCC convicts 288 internet fraudsters

by Friday Olorokor, Abuja

Economic and Financial Crimes Commission claims has secured the conviction of over 288 persons of internet fraud.

The EFCC also said four fugitives were extradited to the United States while another 234 cases were still being prosecuted.

The chairman of the EFCC, Mr. Ibrahim Lamorde, stated this at the commission's Academy in Karu-Abuja during the opening of a three-day conference with the theme: 'Regional Cooperation Against Internet-based Transnational Fraud' on Monday.

The conference is jointly organised by the EFCC and the Australian Federal Police.

Participants at the conference which ends on Wednesday, are drawn from Niger, Sierra Leone, Cameroon, Benin, Togo, Ivory Coast, Guinea Bissau, Senegal, Guinea and Nigeria.

Lamorde put the counterfeit financial instruments seized by the EFCC in collaboration with the Nigeria Postal Service, at \$24m, £858,937 and €1,195, 218,214 respectively.

The anti-graft body boss said, "We must collaborate to at least survive the onslaught and then fight back from the position of strength conferred by pooled resources, shared intelligence, joint operations and other efforts such as this."

Attorney-General of the Federation and Minister of Justice, Mr. Mohammed Bello Adoke, said Nigeria was leading the fight against cyber crime and other economic and financial crimes in West Africa and across the world.

The AGF hailed the Australian Police for collaborating with EFCC in organising the conference.

Adoke said, "While we cannot deny the involvement of some Nigerians in these unwholesome

practices, we vehemently reject the tendency on the part of nationals of some countries even within ECOWAS sub-region to label Nigeria a 419 nation."

The AGF added, "Our law enforcement agencies have recorded giant strides in the enforcement of these laws as evidenced by the increased arrest, prosecution and conviction of internet fraud related offences recorded monthly."

The minister also reiterated the country's commitment to the implementation of all United Nations conventions and protocols in the fight against transnational organised crime.

Special envoy of the Australian Prime Minister to West Africa, Ms. Joanna Hewitt, said she was pleased to attend the conference which, according to her, was indicative of Australia's growing links with Nigeria in recent times.

Here is the URL of the article for as long as it is good:
<http://www.punchng.com/news/efcc-convicts-288-internet-fraudsters/>

419 Coalition comments: Oh, here we go again, Dr. Goebbel's famous 'Big Lie' technique having yet another go round by the Nigerian government. Apparently they just Refuse to learn that, in terms of counter-419 matters, nobody for many years has believed any of their "we're getting the job done" propaganda they put out. The Nigerian government can "vehemently reject the tendency on the part of nationals of some countries even within ECOWAS sub-region to label Nigeria a 419 nation" all it wants to, but that does nothing to change the fact that many people do Indeed label Nigeria a "419 Nation".

And when the Nigerian Attorney General says ""Our law enforcement agencies have recorded giant strides in the enforcement of these laws as evidenced by the increased arrest, prosecution and conviction of internet fraud related offences recorded monthly." We say - What Arrests? What Prosecutions? What Convictions? Do you have a table of these stats posted up on the EFCC website? By date or otherwise? How about a little transparency in these matters, Mr. Attorney General, sir? Where is the confirmable data to back up these assertions of the recent counter- 419 prowess of the Nigerian Government? After all, apparently someone, somewhere, has taken the trouble to add up all these 288 convictions you cite, sir, so how about making all of us privy to that information? How hard can that be? Especially when one considers that 419ing has been a major industry in Nigeria for the last 30 years or so, therefore whoever is assigned to tally up and report on the pitiful 288 convictions over all that time won't exactly be overworked?

And how about all that money and assets the Nigerian government is constantly saying it has recovered from the 419ers? How much of that has actually been paid out to victims of 419? Where is the rest of the money kept? Is it earning interest? Where is that interest being kept? And why does the Nigerian government keep insisting that other countries bust their butts to recover and repatriate monies stolen by Nigerians from the Nigerian people, while simultaneously failing to repatriate significant sums of monies stolen from the citizens of Other countries by Nigerian 419ers? How about a little "Linkage" here, fellas? A little quid pro quo?

Case in point is the Odiawa case of seven or eight years ago when the 419er actually Was convicted, and restitution of over a million dollars was ordered. And here we are, many years later, and the victim has yet to see one thin Dime in restitution, although assets worth several times that which are either owned or controlled by the 419er have been reported. Where is the restitution for the victim? It is long, long overdue. In that same time frame, hundreds of millions of dollars which were stolen from the Nigerian people by corrupt Nigerian officials and such have been repatriated to the people of Nigeria. And the Nigerian Government cannot come up with even a penny of court ordered restitution for the victim in the Odiawa case after all this time. It is absurd. It is things like this which make Nigerian claims of credibility in counter-419 matters a standing joke in the counter-419 community.

If the Nigerian Government truly wants credibility in counter-419 matters, it needs, among other things, to be much more transparent. Post a table on the EFCC website giving the names of 419ers convicted, the date, sentence given, restitution ordered, restitution paid, to whom, and that person's contact info etc. A simple excel spreadsheet could do this, it's not exactly rocket science. We've been asking EFCC to do this for years. What's the problem? Why the resistance? If you guys are doing so great in the counter-419 area, put the info up, trumpet it to the world for All to See and check :)

And in the meantime, how about getting off your collective butts, and in the relatively few cases in which there actually were convictions of 419ers, and restitution ordered (like the famous Odiawa case), how about seizing 419er assets, liquidating 419er assets, and repatriating restitution to the victims of 419ers in a timely fashion? Time to "walk the walk" we and the rest of the world are fed up with decades of the "talk, talk, talk....."

12 MAR 2012
From the Ghanaian Times:

2 Conmen Nabbed By Police

By Matthew Ayoo

The swift response to a distress call by the police on Thursday led to the arrest of two alleged confidence tricksters believed to have defrauded a South African business woman of 200,000 dollars.

In an apparent desperate and confused state, the woman, Joyce Tsitsi, put in a call to the Times

newsroom and asked for assistance to arrest three men who had defrauded her.

The Times called the police who set in motion a hunt for the suspects.

Two of them identified as Steve Watts Owusu and Evans Odoom, were soon located driving in down-town Accra in a sleek four wheel drive and were arrested.

The Accra Regional Police Command are holding the two in custody for questioning while they look for the third suspect named Victor Taylor who claims to be the son of former Liberian Leader, Charles Taylor.

Owusu and Odoom are said to be directors of import/export/mining venture, Tegiva Company Limited.

Narrating her ordeal to the Times, Joyce Tsitsi, said about three years ago she met Victor Taylor who told her that his father had left some gold in Ghana and solicited her assistance to export it to Dubai for sale to sustain him and the family.

She said on their subsequent meeting in Ghana on January 29, 2012 she demanded relevant documentation from him to ascertain the veracity of his claim before she could deal with him.

According to Tsitsi, Taylor produced a statutory declaration allegedly issued by a Notary Public of the Superior Court of Judicature to the effect that he was a Liberian national and owned 215 kilogrammes of alluvial concentrated gold dust deposited with Tegiva Company Limited which was acquired from family resources.

According to her, the statutory declaration also said the gold ore was free from liens and encumbrances, of non criminal origin, and was transferable, exportable and non radioactive material.

In addition Ms. Tsitsi said Taylor produced among other documents, his alleged birth certificate as well as sample analysis and pictures of the gold and the Tegiva company where the alleged gold had been deposited.

She said having been convinced about Taylor's claim, she signed a memorandum of understanding with Owusu, one of the directors of Tegiva which claimed to have stored 215 kilogrammes of gold dust with the purity of 95.33.

Ms. Tsitsi explained that she entered into another agreement with Taylor and Owusu under which the gold dust would be shipped to Dubai and Tegiva company would be entitled to 20 per cent of the total value of the product after it had been exported to the refinery and final assay made to determine the market value.

She said following these agreements, she transferred various sums of money totaling 193,500 dollars to meet the cost of shipment and documentation, cost of storage, test of sample and other incidentals for which Owusu issued receipts in the presence of Odoom, another director of the company.

She said what aroused her suspicion was when the three men failed to meet her demand to see the gold before shipment.

"I became suspicious because after several demands the men could not produce the gold they claimed they have stored for shipment".

Ms. Tsitsi said she also observed that at their meeting, Owusu and Odoom referred to Taylor variously as Samuel, Solomon and Sampson "and that left me with no doubt in my mind that I was being defrauded. I was therefore left with no option but to call for help to report the matter to the police," she said.

Accra Regional Police Command sources told the Times last Friday that caution statements had been taken from the suspects as part of on-going investigations.

Here is the URL of the article for as long as it is good:
<http://www.newtimes.com.gh/story/2-commen-nabbed-by-police>

1 MAR 2012
From CBS3 TV News in Philadelphia, PA sent in by a friend of 419 Coalition:

Summer Renters Scammed At The Jersey Shore

BRIGANTINE, NJ (CBS) A home on Travers Place in Brigantine sounds like a nice to place to rent, according to a copy of the Craigslist ad that offered the three bedroom single family home for \$800 a month.

The problem is the home is only listed for sale by a local realtor. Brigantine police say scammers are using the home's picture and Craigslist to get money from unsuspecting potential renters.

"They are taking a picture of the house from the MLS (multiple listing service) website and they dummy up an ad, it's that simple," said Lieutenant Jim Bennett.

When someone looking to rent responds to the ad, police say the scammer explains by email why the home is available.

"I'm a missionary and I've recently been transferred to Western Africa. Mail or FedEx us your money," Bennett said.

A local couple sent about \$1200 dollars to someone advertising this home for rent for \$800 a month on Craigslist, but never heard back from the so-called landlord. At the time, the home was listed for sale with Coldwell Banker At The Shore.

"They went to the home and noticed we had a sign, so they reached out to the agent to find out what was going on, and the agent was unaware of anything," said agent Colleen Bell.

Police say the couple's money is almost impossible to retrieve from the scammers.

"They're most likely not here in country," said Bennett.

With the summer rental season in full swing, it's renter beware.

"Always use a licensed real estate agent," said Bell

Or meet the home owner at the house for a tour.

"Don't FedEx money, don't send money to anybody, especially out of the country," warned Bennett.

Craigslist offers the same warning and has been removing the ads as they are notified by police.

Here is the URL of the article for as long as it is good:

<http://philadelphia.cbslocal.com/2012/03/01/summer-renters-scammed-at-the-jersey-shore/>

The story was also covered by NBC40 TV in Atlantic City, NJ, here is the URL of that article for as long as it is good:

<http://www.nbc40.net/news/20779/print>

23 FEB 2012

From the Brisbane, Australia Courier-Mail and widely covered elsewhere, sent in by a concerned Nigerian:

Aussie woman scammed Nigerians: court

A BRISBANE woman fleeced Nigerian scam artists by stealing more than \$30,000 from their internet car sales racket, a court has been told.

Sarah Jane Cochrane-Ramsey, 23, was employed by the Nigerians as an "agent" in March 2010 but was unaware they were scam artists, the Brisbane District Court heard today.

Her job was to provide an Australian bank account through which they could funnel any payments they received through their dodgy account on a popular car sales website.

Cochrane-Ramsey was to keep eight per cent of all money paid into her account and forward the rest to the Nigerian scammers.

However, the court heard she kept the two payments she received - totalling \$33,350 - and spent most of it on herself.

The car buyers who were ripped off reported the matter to police, who traced the account to Cochrane-Ramsey.

Police inquiries found her employers were based in Nigeria but had been using a web server in New York to run their dodgy car sales listings.

Cochrane-Ramsey pleaded guilty to one count of aggravated fraud on Thursday.

Judge Terry Martin described her as having a "dishonest bent" after hearing she had a history of stealing and property offences.

He adjourned the sentence to allow her time to provide further details of money she claimed was in a bank account that would allow her to make some repayments.

Cochrane-Ramsey will be sentenced next month.

She was allowed bail until then.

Here is the URL of the article for as long as it is good:

<http://www.couriermail.com.au/news/breaking-news/aussie-woman-scammed-nigerians-court/story-e6freonx-1226279598283>

Here is the URL of the Yahoo News piece on the story, for as long as it is good:

http://m.yahoo.com/w/news_america/blogs/sideshow/australian-woman-turns-tables-nigerian-scammers-17575518.html?orig_host_hdr=news.yahoo.com&.intl=us&

20 FEB 2012

419 Coalition Gives "Props" to International Investigation Services

International Investigation Services, which was based in Iceland but operated worldwide, ceased operations a few years ago.

Under their CEO and founder, Mr. Njall Hardarson, International Investigation Services was the first NGO counter-419 site on the web way back in 1995 or so, several months ahead of 419 Coalition (we were the second).

For a decade and a half, Mr. Hardarson and IIS fought the good fight. Njall was a hands-on counter-419er, a brave man who put himself at personal risk on several occasions in the course of his work.

No-one understands better than 419 Coalition how tedious and frustrating counter-419ing

can be. The work is endless, and the rewards are few.

419 Coalition thanks International Investigation Services and Mr. Njall Hardarson for their pioneering work in counter-419 operations. And you should too.

17 FEB 2012

From the Frederick, Maryland News-Post, sent in by a friend of 419 Coalition:

Embezzlement charges filed

Authorities: Property manager sent stolen money to South African man

By Cara R. Anthony

A property manager in Frederick started wiring embezzled funds to a man in South Africa after the pair developed a relationship on the Internet, according to the Frederick County Sheriff's Office.

Nancy B. Walker, 62, of Boonsboro, served as a property manager for the Ballenger Creek Meadows Home Owner's Association for 15 years, according to Cpl. Jennifer Bailey of the sheriff's office, who said Walker stole \$137,000 in about two months.

"Walker was romantically involved with a man that she met on the Internet," Bailey said. "The investigator did not provide the name of the website where they initially met, but said the two had a lot of contact through instant messaging, email and phone conversations and that they never met in person."

Authorities charged Walker on Wednesday on a criminal summons with one count of theft scheme over \$100,000, one count of theft \$10,000 to under \$100,000, and 40 counts of theft over \$1,000.

It is unclear whether Walker sent the total sum to her romantic interest, but she did send money to South Africa more than once, the sheriff's office said. Numerous unauthorized withdrawals were made from two bank accounts for about two months before the association's board members noticed.

The association reported Jan. 27 that unauthorized withdrawals were made from their bank accounts. Those accounts were managed by Association Management Services Ltd. on Thomas Johnson Drive in Frederick, the release said.

A two-week investigation revealed that from Nov. 23 through Jan. 23, Walker stole money from the association. After obtaining a warrant, authorities linked some of those funds to South Africa.

"The man told Walker that he needed financial help and she wired the money to locations that he provided in South Africa," Bailey said.

Investigators obtained two search warrants Jan. 31, one for Association Management Services Ltd., the other for Walker's home in Boonsboro, the release stated. Evidence related to the case was seized.

The Maryland Homeowners' Association, a nonprofit homeowner advocacy group, said there are ways small homeowner associations can protect themselves from embezzlement.

"Management companies must never have sole control of the association's money," said Jeanne N. Ketley, the nonprofit's president. "The treasurer must critically review the monthly budget reports."

Here is the URL of the article for as long as it is good:

<http://www.fredericknewspost.com/sections/news/display.htm?storyID=131954>

WBAL-TV in Baltimore, Maryland also covered the story, here is that URL for as long as it is good:

<http://www.wbaltv.com/news/30482776/detail.html>

15 FEB 2012

From the Nigerian newspaper The Punch:

British divorcee loses 40,000 UK Pounds to Nigerian fraudster

by Agency Reporter

A divorcee was tricked into sending £40,000 to a Nigerian fraudster she met over the internet.

Vicky Fowkes, 59, decided to start dating online in early summer 2010 and by August she was sending money through 'moneygrams' to a man in Nigeria she believed was a charming Briton called John Hawkins.

By November 2010 the man, who claimed he was an engineer with his own property business, had received nearly £40,000.

But Fowkes' hope of love was shattered when the police visited her home in Tewkesbury, Worcestershire, and revealed the romance was a scam concocted by an internet fraudster.

The mother-of-two said, "I put my trust in this person and I was beginning to start a relationship with him, but now the whole affair has had a devastating effect on my life. I have been humiliated and have lost my self-respect."

Fowkes, a self-employed child care consultant, began sending money to Nigeria in August 2010 after

her internet lover failed to visit her at Heathrow after telling her he had booked a flight.

She told Telegraph.co.uk, "He was due to come for a visit in August but he wasn't on the flight and then when he rang later that day he said they stopped him at customs to do with tax issues with his business. Two weeks later he started asking me for money."

The man masquerading as John Hawkins claimed he was being fined by the government for the tax that he owed.

But West Mercia Police visited Fowkes and broke the news that she was the victim of a fraudster.

Robin Longmore, a financial intelligence development officer for West Mercia Police said, "Through our investigations we started to believe Vicky was a victim. This kind of thing is a massive problem in Nigeria and Ghana with groups of men sitting in internet cafes all conning people over their internet dating sites."

"We believe that this person was operating from Nigeria and John Hawkins is clearly a made up name and the pictures that he used are obviously taken from the internet and are innocent members of the public."

Here the the URL of the article for as long as it is good:

<http://www.punchng.com/metro/british-divorcee-loses-40000-to-nigerian-fraudster/>

13 FEB 2012

From the Nigerian newspaper, The Punch:

Nigerian arrested for online lottery fraud

by Agency Reporter

A Nigerian, Paul Osagie, was among three persons arrested by the Chennai Police in Bangalore, India on Thursday in connection with an online lottery fraud, police sources have said.

Based on a complaint lodged by Dinesh Kumar (21), a third year engineering student of a private university, that he was swindled of Rs. 1.34 lakh by unidentified persons after he responded to an online lottery prize sent through text message, a special team of the Central Crime Branch was formed to investigate the matter.

The complainant said that he received a text message, that he had won \$2m in 'yahoo-msn lottery draw'.

When he replied to an email address given in the message, a man claiming to be a diplomat in the United Kingdom responded, saying that the prize money would be delivered in India, he asked Kumar to deposit Rs. 1.34 lakh in two different accounts of ICICI Bank.

The money, the accused said, was for local taxes and customs clearance.

After Kumar deposited the money, it was drawn in an ATM centre in Bangalore. The accused called back from a mobile number and said Rs. 3 lakh more had to be deposited in the same accounts towards airport charges. Suspecting foul play, the student lodged a complaint with the Commissioner of Police J.K. Tripathy.

"This is yet another case where bank accounts and SIM cards activated with bogus documents become effective tools in the hands of culprits. Video footage at an ATM centre in Bangalore showed two persons drawing the money."

"Following specific clues, the team arrested Osagie (41), and his associates Mohamed Afzal (29) of Mumbai and Rajesh Viswanath Kedia (49) of Kolkata. Rs. 94,000 was recovered from the possession of Cyril," Additional Deputy Commissioner of Police M. Sudhakar said.

Here is the URL of the article for as long as it is good:

<http://www.punchng.com/news/world/nigerian-arrested-for-online-lottery-fraud/>

3 JAN 2012

From BBC News, sent in by a concerned Nigerian:

'Spam capital' India arrests six in phishing probe

Every month, Indians are adopting the internet in their millions - but growth is attracting crime

Police in India say they have arrested six foreign nationals suspected of defrauding hundreds of people using text message and email scams. Scam victims were duped after being told they had won a lottery.

Authorities seized 14 laptops, seven memory sticks and 23 mobile phones, as well as fake documents and cash.

The arrests come after security firm Kaspersky reported that India now sent more spam than any other country in the world.

Police said the six men, all Nigerian, would be remanded in custody until 12 January.

The arrests signal attempts to crack down on a growing cybercrime problem in the region.

Mumbai-based internet security specialist Vijay Mukhi said poor enforcement of laws meant spammers could act with impunity.

"We have an Information Technology Act that was introduced in 2000. But we don't have any convictions under it and it's silent on spam," he said.

"If I'm a spammer, I would rather spam from India to India and the rest of world because nothing will happen to me."

Free reign

In its report, Kaspersky said 14.8% of all spam email sent in the three months prior to the end of September had originated in India.

Darya Gudhova, Kaspersky's spam analyst, said a lack of security awareness had given spammers free reign.

She added that there was a growing level of cybercrime activity in developing regions such as Asia and Latin America.

The Internet and Mobile Association of India (IMAI) estimates that the country has more than 112 million internet users, the third largest in the world after the US and China.

About seven million new users are being added every month, the IMAI said.

David Emm, a security researcher from Kaspersky Labs, said this growth was making life difficult for the authorities - but believed the arrests signalled a strong sign of intent from the Indian government to get a grip on scammers.

"One of the good things is that they are taking it as a serious issue," he told the BBC.

"Cybercrime activity is breaking out of the western European theatre and starting to affect other parts of the globe because of the massive growth in IT. [In Europe] we've had cybercrime legislation for a long time with lots of expertise and history of dealing with it - but if you go to other areas like Brazil or India, you find they don't necessarily have specific cybercrime legislation."

[Go To 419 Coalition Main Page](#)

[Go To 2018 News](#)

[Go To 2010 News](#)

[Go To 1999 News](#)

[Go To 2017 News](#)

[Go To 2009 News](#)

[Go To 1998 News](#)

[Go To 2016 News](#)

[Go To 2008 News](#)

[Go To 1997 News](#)

[Go To 2015 News](#)

[Go To 2007 News](#)

[Go To 1996 News](#)

[Go To 2014 News](#)

[Go To 2006 News](#)

[Go To 2013 News](#)

[Go To 2005 News](#)

[Go To 2012 News](#)

[Go To 2004 News](#)

[Go To 2011 News](#)

[Go To 2003 News](#)

[Go To 2002 News](#)

[Go To 2001 News](#)

[Go To 2000 News](#)