

In the press

Nigerian scam update: The crackdown continues

Not sure why, but I seem to be on the receiving end of a regular barrage of extortion letters lately as well as a load of 'Ezines', most of which go straight into the recycle bin -

- However a newsletter from a company called Westcom contained these tit-bits which caught my eye.

Paragraph four on the Nigerian scam contains information that deserves to be in Ripley's 'Believe it or Not'!

*- Are people really this gullible?
- AM*

What's being done to fight this fraud and how big a problem is it really?

In the past Westcomm News have published a series of articles about the notorious Nigerian email fraud - know as the 419 scam - in which victims are offered a share of a vast fortune in return for allowing the money to be laundered through their bank account.

Many people have read coverage and a lot of people have sent replies to various media with their own stories of these fraudulent emails, expressing concerns about what is being done to crack down on this crime.

Edward Venning, spokesman for The National Criminal Intelligence Service, an organisation which works on behalf of UK law enforcement agencies with a remit to investigate these kinds of scam, said: "For the past 18 months we have been receiving around 1,000 emails per week reporting these scams and we are constantly working to collate the intelligence from these emails. "From the intelligence we have gathered from victims of this fraud we were able last year to secure 24 arrests and convictions in South Africa and 12 in the UK."

Furthermore, according to Venning, the UK is one of only two countries in the world dealing with this problem so proactively, with the other being the US through the Secret Service. To put the problem into perspective, last year alone 150 people were victims of this fraud, according to NCIS figures. [The average amount of money lost by these victims was GBP56,675](#) - a figure boosted by the fact that a

couple of victims were already millionaires before being tempted by the fraudulent 'get-rich-quick scheme'.

While many of these victims will find sympathy hard to come by, Venning countered the suggestion that these scams are undeserving of lengthy, and costly investigation, explaining that the problem is far more serious than a few fools being easily parted from their money. According to Venning, the unwitting individuals who hand over their bank details to these scammers are directly funding the trafficking of Class A drugs into Europe from Africa as well as other activities such as car crime. And Venning believes there is still much more which needs to be done - starting with the ISPs, the main conduit nowadays for 419 correspondence. He said: "ISPs in general are adopting a 'head in the sand' attitude towards this problem."

But the victims in all this aren't only those in Europe or the US who are receiving the emails. It's likely the close association with fraud has irreparably damaged the reputation of Nigeria. "From a business perspective this scam reflects very badly upon Nigeria as a country," said Venning, adding that the Nigerian High Commission has worked very closely with NCIS to crackdown on the handful of individuals whose actions have tarnished the country's image.

The problem is now moving further away from its roots in Nigeria as a result of the notoriety this scam has achieved.

According to Venning, Nigeria has now used up its "trust capital" - meaning it is now so inextricably linked with fraud that emails from within the country are almost always regarded with suspicion. As such many of the fraudsters are decamping to South Africa.

Where is the University of Palmers Green?

US federal authorities and Enfield Trading Standards have shut down a number of websites selling bogus degrees and driving licences, recovering more than US\$6m

The websites sold degrees from non-existent UK universities, such as the University of Palmers Green and the University of Devonshire, and fake international driving licences. Although buyers knew the degrees and licences were bogus, employers in other countries, particularly the US, were apparently taken in by them.

The alleged operators of the websites, a couple with joint US/Israeli citizenship, are said to have run the racket from Romania and the US. The operation was given credibility by the use of a London mailing address and a staff of two based in north London to forward their mail.

Tony Allen, an investigator with Enfield Trading Standards, said that the business and its clients were relying on overseas employers being impressed by the

general good reputation of UK universities while knowing little of the individual institutions. He said the result was unqualified people obtaining jobs in sensitive occupations such as teaching and working with children. Enfield Trading Standards started their investigations approximately four years ago after receiving complaints from employers trying to follow up references. "An investigation normally wouldn't take this long but this was a very complex case," said Allen. "We had to identify where the gang was based by identifying the Internet protocol addresses.

"It wasn't until we started dealing with the Federal Trade Commission that we were able to trace these and the bank accounts, which have been frozen by the Americans." No criminal charges can be brought by Enfield, which, to get the websites closed, had to cite civil procedures and argue that the sites were not in consumers' best interests. "It's difficult trying to prove deception," said Allen. "The people who bought the degrees knew they were false, so in fact they were doing the deceiving rather than being deceived."