News

Download this release at k-state.edu/media

K-STATE Kansas State University

Media Relations
9 Anderson Hall
Manhattan, KS 66506-0117
785-532-6415
Fax: 785-532-6418
E-mail: media@k-state.edu
k-state.edu/media

**Source:** Harriet Ottenheimer and Davi Ottenheimer, mahafan@k-state.edu, davi@poetry.org. http://www-personal.ksu.edu/~mahafan/
**News release prepared by:** Greg Tammen, 785-532-6415, media@k-state.edu

*Wednesday, April 7, 2010*

**EXPERTS SAY RESEARCH INTO NIGERIAN 419 SCAM E-MAILS COULD LEAD TO IMPROVED ANTI-PHISHING TECHNOLOGIES, MOST MESSAGES NOT ACTUALLY FROM AFRICA**

MANHATTAN — Chances are you have received one at some point or another: an e-mail from someone in Africa asking for your help or informing you of a large inheritance from a deceased relative. Whatever the scenario, the sender always asks for a financial contribution. Thanks to the research of a former Kansas State University professor and her son, spam e-mails of this type may soon be a thing of the past.

For seven years, Harriet Ottenheimer, a K-State professor emeritus of anthropology and a Fulbright scholar to the Czech Republic, and her son, Davi Ottenheimer, president of security consultancy flyingpenguin, collected and analyzed Nigerian 419 e-mails for clues that could be used to block these messages. These spam e-mails are called Nigerian 419 messages, or 419 for short. The number "419" refers to an article of the Nigerian Criminal Code concerning fraud.

Typically the messages ask for the recipient's help to facilitate a financial deal. The recipient/victim is asked to pay an advanced fee to set up an account with the promise of a larger reward at the end of the transaction. If the victim pays the initial fee, the sender/scammer says that a problem has arisen which requires additional funds, beginning a never-ending cycle of payments until the victim realizes they've been scammed.

By carefully analyzing the linguistic patterns in the e-mails, the Ottenheimers believe a technological solution can be created for e-mails to automatically be scanned and alert the recipient if there appears to be a possibility of fraud, thereby improving the anti-phishing technologies. The result would be similar to how anti-virus software scans for bad code in viruses and malware.

Ottenheimer used her linguistic skills to decode the discourse of the scam e-mails and how they work on their victims. Primarily, she said, the victims have been well-educated westerners, such as such university professors, doctors, lawyers, financial planners and bankers.

According to their research, slightly fewer than half of the e-mails could be successfully traced to Africa, whereas slightly more than half of the e-mails could be traced to places like Eastern Europe, the Middle East, Asia, the United States, North America and South America.

(more)

"The main point is that 'African' scam letters are written so as to appear to be from Africa. There are other kinds of scam letters purporting to come from other places and the language in those is tailored equally carefully to appear to be from those places," she said. "You can't really tell who is writing the letters, or where they are situated in the physical world, but if you are going to write a letter and claim to be a Russian engineer, or a Burmese princess, or a Middle Eastern widow of an oil-man, or the son of a Nigerian dictator, then you will probably want to choose your linguistic style carefully so that you sound 'authentic' to the recipient."

The Ottenheimers intend to publish their findings as well as continue to look for linguistic patterns that can be used as a component of technological solutions to counteracting Internet fraud and improving security systems.

To date, the 419 Coalition, an organization devoted to educating the public about the scams, reports that as of 1996, the scam has accounted for $5 billion in stolen money worldwide.

#