Beware the sophisticated 'spam zombies' to come

By DAWN WALTON
THE (TORONTO) GLOBE AND MAIL

CALGARY, Alberta -- Unless new weapons are designed to keep junk mail at bay, spammers are about to get the upper hand in the war in cyberspace.

Canadian researchers have figured out a way to create spam that could bypass the best filters and trick even the most savvy computer users into opening messages they would normally delete.

Mischief makers would use this kind of spam -- which employs hijacked computers to make sophisticated e-mail messages that appear to be from people known to computer users -- to release viruses, worms or spyware on unsuspecting users or expose them to theft of personal information.

"It's very much an arms race between the good guys and the bad guys," said study co-author John Aycock, a computer scientist at the University of Calgary.

Spam is always evolving, but the kind of high-tech stuff once thought to be too much work for spammers was easily demonstrated by Aycock and student-researcher Nathan Friess in their study, "Spam Zombies from Outer Space."

The study was financed by the Natural Sciences and Engineering Research Council of Canada.

Alex Leslie, vice president of technology for AOL Canada, said the researchers have hit upon something that Internet service providers are always trying to prepare for: threats they anticipate, but have yet to see, known as a "zero day attack."

"It's a never-ending battle. It's a cat and a mouse game," Leslie said.
Beware the sophisticated 'spam zombies' to come

Those tricks would make sure people are more apt to visit a Web link or download an attachment, allowing the spammers to peek into hard drives, grab personal data or infect the computer.

The majority of spam is sent through zombie computers, which are vast networks of hijacked personal computers infected by rogue software, which is used to send bulk e-mail messages.

But the researchers found that zombie computers could be harnessed in a new way, which they showed using two computer programs as well as manually inputted e-mails and e-mail lists from the Enron database, which was released when the company went bankrupt.