

Confidently secure and control access with Juniper Networks.



'Money Mules' Increasingly A Cog In Cybercrime Underground

With phishing scams on the rise, one expert says cybercriminals need to recruit 10,000 to 20,000 people a year to help illegally transfer money out of victims' accounts.

By Sharon Gaudin, [InformationWeek](#)

Aug. 24, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=201802255>

This week's news that malware authors are soliciting people to be "money mules" comes as no surprise to security researchers, who say it's a burgeoning trend in the cybercrime underworld.

"It's been going on for a while, but we're seeing it increasing," said Gunter Ollmann, director of security strategy at IBM's Internet Security Systems, in an interview with *InformationWeek*. "The average life of a mule appears to be fairly short. ... But the phishers haven't stopped using them. They just need more mules."

[Money mules](#), also called phishing mules, basically are the middlemen for phishers or hackers trying to raid compromised bank accounts. The phisher gets the necessary personal and financial information to access the victim's bank account and then turns to the mule, who generally has his or her own account at the same bank. The mule accesses the account with the stolen information, transfers money to the mule's own account, then keeps a certain percentage and either wires or transfers the remaining balance to the phisher.

Experts theorize that cybercriminals use the mules because banks are increasingly watching for bank transfers, especially large sums moving out of the country.

Ollmann estimates that between 2% and 4% of phishing scams are successful. That means hundreds of thousands of people and their bank accounts are victimized every year -- and he figures between 10,000 and 20,000 of those thefts use mules to transfer the money.

The case that received attention this week involved the malware authors behind the Prg Trojan apparently [soliciting their own identity theft victims](#) to become money mules. The hackers have stolen countless identities and pieces of bank account information by embedding the Trojan in an advertisement that ran on online job sites. Symantec's Security Response team reported discovering templates of e-mails that the Trojan authors are sending out, using their newly acquired collection of stolen identities to target their money mule scam at people looking for jobs.

While the e-mail says the job -- such as the position of "Transfer Manager" -- doesn't require any experience and offers a \$500 sign-on bonus and the ability to work from home, it also notes that it does require people to have an account with Bank of America for wire transactions.

Graham Cluley, senior technology consultant with Sophos, said in an interview that phishers and hackers often prey on people who need to make some extra cash quickly and easily.

"We've seen gangs trying to recruit mules, appealing to working moms and the like, saying they can make loads of money from home," he said. "Some people don't know what they're involved in and are just being manipulated. Others do know what's going on and are willingly helping squirrel money out of the country."

Ollmann said a lot of the mules -- many of whom are students -- may not know that they're involved in money laundering.

"They're being promised that they can work for an hour or two a day and earn thousands a month. They only have to live in the U.S., use this bank, and work from home a few hours a day," he added. "A lot of the spam you receive is recruiting mules. When it says work from home and earn \$5,000 a month, that's probably a recruitment. The Web sites they use are actually very commercial. They look like legitimate companies and recruitment sites. A lot of these sites have been up for months if not years and they look very professional and they easily take people in."

Don't touch it. Don't replace it.

Copyright © 2007 [CMP Media LLC](#)