
Spammers Make a Sound Investment in Stocks

Unsolicited e-mail that touts penny stocks is on the rise and getting results.

By Tyler Hamilton

A new study reveals that spam messages promoting stocks can make you money -- if you're the spammer.

"Hot Energy! Oil Stock!" shouts the typical message. "Ready To Run!! Big Winner!!! Huge Advertising Campaign This Week!" Such come-on messages often refer to a company with a listing on the [Pink Sheets](#), an over-the-counter stock quotation system. They're designed to entice novice traders to buy stocks that are normally overlooked.

These annoying campaigns are growing in frequency and volume. [Sophos](#), a Massachusetts-based supplier of software for protecting companies and consumers from online threats, reported in July that 15 percent of all junk e-mail messages are now stock spam, up dramatically from less than 1 percent 18 months ago.

So why is stock spam on the rise -- and adapting quickly to technologies designed to stomp it out?

"It's not that it's just cheap to send, but it actually gets results," says [Jonathan Zittrain](#), professor of Internet governance and regulation at Oxford University, and co-author of a new study, "Spam Works: Evidence from Stock Touts and Corresponding Market Activity." He's also co-founder of the [Berkman Center](#) for Internet & Society at Harvard Law School.

Stock spam uses the classic "pump-and-dump" scheme. A spammer sends out a mass e-mail message touting a penny stock with low trading volume in hopes of convincing a handful of people to buy shares of it. If the spammer succeeds, the limited buying activity boosts the stock's price and liquidity just long enough for the spammer to sell his own shares (or the shares of his client) at a profit. The stock subsequently plunges and those who bought it are usually hit with a loss.

In their study, Zittrain and co-author [Laura Frieder](#), an assistant professor of finance at Purdue University in Indiana, sought to quantify the effectiveness of such campaigns.

To do so, they analyzed more than 75,000 stock "touts" appearing in Zittrain's e-mail inbox and a Usenet spam-sighting newsgroup between January 2004 and July 2005. The date and estimated size of each spam campaign was compared with the price and trading volume of the company shares being promoted over several days, including the day immediately preceding the campaign.

The researchers discovered that if a spammer bought a stock a day before beginning heavy touting, then sold the morning after the first day of touting, the average return on investment was 4.9 percent. And more effective spammers saw a 6 percent return.

On the other hand, if a victim were to invest \$1,000 in a stock on the day of heaviest touting, that investment would be worth, on average, \$947.50 in the two days following the spamming campaign. For the most heavily touted stocks, the same investment would fall by 7 percent, to \$930. The study also confirmed that the volume of touted stocks responded "positively and significantly" to touting campaigns, meaning that trading activity increased.

"Our analysis shows that [stock] spam works," wrote Zittrain and Frieder. "Among its millions of recipients are not only those who read it, but who also act upon it, suggesting a value to spamming that will create a powerful counterbalance to regulatory and technical efforts to contain it."

Containing it has definitely proven to be tricky. Such e-mail spam messages are spreading like wildfire, helped by Trojan viruses, which can assemble armies of "zombie" computers to disseminate spam on command.

To make matters worse, more stock spammers are embedding their messages in digital images, making them invisible to text-based software filters. And even filters that can scan images for digital signatures are easy to fool.

"By making small alterations in the pixels of the image, they're able to obfuscate the image," says Ron O'Brien, senior security analyst at Sophos. Spam containing images accounted for 35.9 percent of all spam in June, up from 18.2 percent just six months earlier, according to the company.

"The thing that surprises most people is that the company [whose stock is being touted] is often not aware their shares are being manipulated in this way," adds O'Brien.

"They're often just as much the victims."

Gordon LeBlanc Jr., founder and chief executive officer of Phoenix-based PetroSun Drilling, describes himself as just such a victim. He says he had never heard of stock spamming until a spammer began touting shares in his oilfield services company in early July. Since then, the complaints have been rolling in.

"I'm not a happy camper," says LeBlanc, who was hit most recently in mid August. "It's been going on sporadically for about a month and a half. It's very frustrating. It seems they'll do it for every press release we put out."

Like dozens of other companies listed with the Pink Sheets, PetroSun was forced to issue a press release explaining that its shares were being manipulated by an unknown third-party spam campaign.

The problem has become so widespread that Pink Sheets LLC issued a proposal to the Securities and Exchange Commission in April urging the regulator to impose stricter rules on stock spammers, such as forcing them to reveal their identity and intent in e-mails and requiring the spammers to provide the issuer of the stock with a copy of their promotional e-mail. The SEC has yet to take action.

But O'Brien says disclosure rules will never work, largely because most spammers won't comply with the law. He's also not so sure that better information campaigns will enlighten the public enough to stop the effectiveness of stock spamming.

"This is about greed. Frankly, this is a form of gambling," says O'Brien, adding that there will always been a percentage of the population attracted to a pump-and-dump scheme in hopes of beating the odds.

But Zittrain points out that even gamblers have rules to protect them, and that it may be time for regulators to consider more aggressive -- even paternalistic -- applications of the law to protect those more susceptible to stock spam.

One possibility is to introduce steps, or "speed bumps," in the brokerage trading process that would prevent the recipient of a stock tout from immediately acting on it, says Zittrain, adding that such a "cooling off" period might make a person think twice.

Brokerages could also be supplied with a "neighborhood watch" service that alerts them to the most recently discovered stock spam campaigns. If a client calls and places an order for a recently touted stock, a red flag goes up and by law the brokerage

intervenes with a warning.

"It wouldn't be that difficult to set up such an early warning system," says Zittrain.

Copyright Technology Review 2006.