FEATURE

PREDICTIONS ABOUT THE PREDICTION SCAM

Sampson Pun, Eric Parsons, Margaret Nielsen, David Ma and John Aycock
University of Calgary, Canada

Many traditional confidence games have made their way into electronic form. Witness the humble advance fee fraud, for example, dating back to before Jack the Ripper's time [1, 2] and now flourishing in large volumes thanks to the magic of spam. One scam that is conspicuous by its electronic absence, however, is the prediction scam.

The prediction scam works like this. A scammer picks an event with a typically binary result, such as a sports event: win or lose. Starting from a pool of (say) 32 people, the scammer contacts half the people and predicts one result, predicting the opposite result to the other half. The event occurs, and the scammer must have given the correct prediction to 16 people. Those 16 are now split into two groups, and the scammer repeats the process, and then repeats the process again. Now four people are really, *really* convinced of the scammer's predictive powers.

The scammer makes money by asking people in the final group to pay for the next prediction. Remember, this group has only seen correct predictions from the scammer, so the likelihood of them being willing to pay is fairly high. The victims expect to recoup their investment by betting on the event themselves. Of course the paid-for prediction, if it arrives at all, is no better than a random guess.

It is easy to imagine this scam electronically: the scammer turns spammer, and emails the predictions to the masses. The problem with a naïve conversion of the prediction scam into electronic form is time. The scammer must remain able to contact and hold the interest of their potential victims for long enough to make the predictions, and for the corresponding real-world events to occur. This can be mitigated somewhat by choosing periods when lots of events are happening, such as sports playoffs. However, the time factor still means there is a real risk to the scammer that their emails will become blocked as spam.

The answer comes in the form of *parlaying*. In gambling, a parlayed bet is made on the outcome of multiple games; the bet is only won if all the games turn out as predicted. Now, instead of having to get N prediction emails through to a victim, the scammer sends one email containing N predictions. To people who get the correct predictions, the scammer has instant credibility after just one spam run.

Now, the scammer has two choices for the victim to make contact. They can continue to use email because the situation has changed, and not in favour of anti-spam. The relatively small number of victims' emails can now be handled manually by the scammer, so there are no giveaway bulk mail indicators. Furthermore, the victim now *wants* the scammer's emails, and it is not far fetched to imagine the scammer asking a victim to adjust their anti-spam filter accordingly.

The scammer could also send the victim to a website. This means that anti-spam defences only get one chance to detect this fraud, at the outset. A clever scammer would also make the website require login, and issue unique logins for each prediction; only the people who receive correct predictions are allowed into the site.

At the scammer's website, the victim would buy the next prediction, or buy some software that they can use to make their own predictions. The latter, of course, is an opportunity for the scammer not just to make money, but to infect the victim's machine. Browser-based anti-phishing defences could block access to the scammer's website if the scam is caught in time, but again the victim wants the scammer's communication – anti-phishing defences may quickly find themselves disabled.

The prediction scam is not limited to sports. Stock predictions work equally well [3, 4], and may even lead to a new variant of the pump-and-dump scam. After all, who wouldn't listen to a STRONG BUY stock alert from someone with a proven ability to predict the stock market?

The prediction scam is unfortunately likely to be successful when it makes the transition into electronic form. To start, users will simply not be wise to the scam. Also, unlike advance fee fraud, there is no need for the scammer to build their credibility or convince the victim, because the 'proof' is already supplied and is independently verifiable. Throw away the crystal ball and Tarot cards: the future of prediction is on its way.

REFERENCES AND NOTES

John Aycock's research is supported in part by the National Sciences and Engineering Research Council of Canada. He thanks Kelly Wilson for some fact-checking.

[1] Power-Berrey, R. J. The bye-ways of crime: with some stories from the Black Museum. Greening, 1899.

[2] Letter from Foreign Office (signature illegible) to the Under Secretary of State of the Home Office, 22 February 1881. In UK National Archives, HO 45/9606/A2527.

[3] Paulos, J. A. Innumeracy: Mathematical illiteracy and its consequences. Hill and Wang, 2001.

[4] Henderson, L. Crimes of persuasion: Schemes, scams, frauds. Coyote Ridge, 2003.