Breaking the Fourth Wall of Electronic Crime: Blame It on the Thespians

Hal Berghel
University of Nevada, Las Vegas

Actors and electronic criminals are both in the business of perception management and social engineering, and they have similar motives as well: getting their audiences to suspend disbelief.

I have been conducting research in cybercrime for several decades and am frequently asked to speak on the subject. Understandably, academic and student groups tend to be more interested in the technical side of cybercrime—Web hijacking, SQL injection, and the like. But the more popular topics for general audiences include transnational money laundering, the structure of shadow economies, criminal communities, and kleptocratic states.

The more general talks are actually the more important ones, for the technical side of electronic crime tends toward the lowbrow and uninspired, and there's a multitude of variations on themes. For that reason, whatever the specific topic, I like to begin my talks by paying homage to the progenitor of online computer crime: the Nigerian 419 scam. Known by that name because 419 is the section of the Nigerian criminal code that deals with cheating, this scam is majestic in its simplicity. No password cracking involved. No sophisticated electronics. No zombie computers. No malware. All that's required is an e-mail account, webserver access, and a criminal mind.

The Nigerian 419 scam's strategy dates back hundreds of years to the Spanish Prisoner', a confidence trick in which a mark in search of a fast buck is enlisted to "advance" funds to help gain the release of a person of considerable means who has run afoul of the law (or some variation thereof), with the hope of being richly rewarded for the good deed. Modern embodiments of this confidence trick fall under the rubric of "advance-fee frauds," which to this day are among the more popular confidence schemes.

I find it incredible that this scam has succeeded for such a long time. After all these years, variations on the theme, replete with misspellings and egregious grammar, still surface. This longevity testifies to the fact that there are still enough potential victims to make it profitable. While this scam doesn't have the criminal appeal it once had, it doesn't take many victims to justify the effort when e-mail is free to the sender, and the source country's legal machinery is focused on prosecuting political dissidents and the disenfranchised.

The Nigerian 419 scam was successful because it tied together the essential elements of electronic crime: perception management, social engineering, and technical subterfuge. Thinking this is a legitimate, personal appeal for help that appears not too unreasonable, the victims are manipulated into doing something they wouldn't normally do—like sending checks to strangers in Nigeria.

 Published by the IEEE Computer Society

In many ways, the technical subterfuge—all you need is an e-mail account and a friend who can hack out some basic HTML—is the least interesting aspect of this scam. This holds true for many other forms of electronic fraud and crime.

PLACING THE BLAME WHERE IT BELONGS

It's time that we technologists place the blame for phishing and electronic crime squarely where it belongs: actors. The Nigerian 419 scam owes its success to performers.

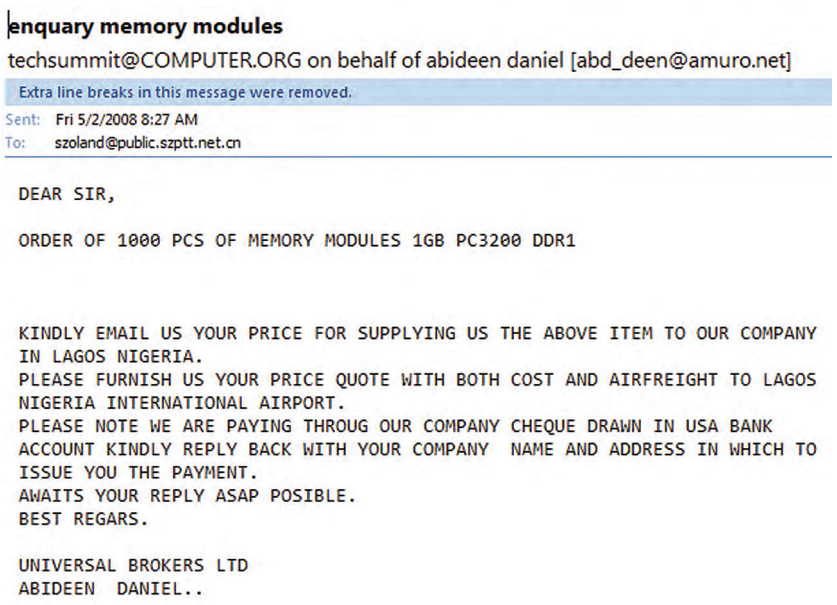
Actors and other members of the broader literary and performing arts community engage in storytelling. Criminals learn by example—the big screen, the little screen, and, in the case of the long-in-tooth, radio. The talented performers, playwrights, novelists, and poets among us must accept responsibility for their contributions to criminal behavior. Although they might not label it as such, they're in the business of perception management and social engineering.

The contribution of audiences, readers, and victims is the willing suspension of disbelief. If done well, the audience/victim becomes the proverbial putty in the hands of the actor/criminal. Credit for a perfect Ponzi scheme owes less to Bernie Madoff and Tom Petters than to Julia Roberts and Tom Hanks. We can't solve these problems by beefing up the reading lists in B-schools.

Preventive measures must be taken in theater troupes and literature classes Perception management is the ability to trick people into thinking they perceive or experience something they actually don't—or to not perceive something when they really do. Contrary to popular belief, the art of perception management did not begin with military PSYOP programs, advertising agencies, or polemicists who pose as journalists on cable TV.

This art form arose in the theater. Actors have successfully used perception management techniques for thousands of years. I'm confident that audiences in pharaonic Egypt knew full well that the children onstage weren't really going to die from the famine but were moved to sorrow nonetheless. Similarly, a carefully crafted and effectively presented soliloquy that moves the audience to tears is an act of social engineering.

Technologists tend not to give the broader artistic community its just desserts in this regard. Perception management and social engineering are not something that Kevin Mitnick or the Hewlett-Packard pretexting scandal introduced to our culture. They've been around as long as we've had wordsmiths and orators.



enquary memory modules

techsummit@COMPUTER.ORG on behalf of abideen daniel [abd_deen@amuro.net]

Extra line breaks in this message were removed.

Sent: Fri 5/2/2008 8:27 AM

To: szoland@public.szptt.net.cn

DEAR SIR,

ORDER OF 1000 PCS OF MEMORY MODULES 1GB PC3200 DDR1

KINDLY EMAIL US YOUR PRICE FOR SUPPLYING US THE ABOVE ITEM TO OUR COMPANY IN LAGOS NIGERIA.
PLEASE FURNISH US YOUR PRICE QUOTE WITH BOTH COST AND AIRFREIGHT TO LAGOS NIGERIA INTERNATIONAL AIRPORT.
PLEASE NOTE WE ARE PAYING THROUG OUR COMPANY CHEQUE DRAWN IN USA BANK ACCOUNT KINDLY REPLY BACK WITH YOUR COMPANY NAME AND ADDRESS IN WHICH TO ISSUE YOU THE PAYMENT.
AWAITS YOUR REPLY ASAP POSIBLE.
BEST REGARS.

UNIVERSAL BROKERS LTD
ABIDEEN DANIEL..

Figure 1. A recent phishing scam that appears to have come from someone who spent too much time watching grindhouse films.

ROY ROGERS AND THE WILLING SUSPENSION OF DISBELIEF

I live and work in the greatest city in the world—Las Vegas. It has almost everything. And what it doesn't have (like an ocean) can be found in our suburbs, such as Los Angeles. Until just a few years ago, in between the two was the Roy Rogers Museum in Victorville, California.

Roy was huge in my day, so when traveling to L.A. with my kids, we used to visit the museum in honor of Roy, Dale, Pat, Andy, Gabby, and the crew. On one occasion, I bought a boxed set of DVDs of the old Roy Rogers TV shows. My youngest, about six or seven years old at the time, agreed to watch one of the DVDs with me—a level of cooperation my teenagers were unwilling to match. About a minute into the experience, he said, "Dad, there's something wrong with the color." I pointed out that all TV was black-and-white in those days, and that it was actually better without color. He was having none of it.

However, being both a parent and an academic, I couldn't let the matter rest there. I followed up with a treatise on how the human mind is so powerful that it can make up for perceptual shortcomings—like the lack of color. Before black-and-white talkies, I explained, there were silent movies where the audience couldn't hear the actors speak. They had to read what was said on intertitles while a piano player or organist sitting in the front of the audience provided musical accompaniment. But audiences got just as much enjoyment from them as

we do now, I counseled. Colorization, special effects, big screens, surround sound, and the like are superfluous extravagances, pure and simple. My son listened politely, but my concept obviously wasn't resonating with him, and, alas, I lost my viewing partner.

Of course, my point is that our minds engage the theatrics at whatever level of intensity is offered. The reason is a phenomenon that successful actors, playwrights, novelists, poets, and storytellers of every stripe have internalized over thousands of years: the willing suspension of disbelief. That's really all it takes to get victims to start writing checks to Nigerian banks.

REMEMBER: ACTORS AND CRIMINALS HAVE SIMILAR MOTIVES

So the next time you're asked to do some forensics on a phishing attack like the one shown in Figure 1, don't try to analyze it in terms of port-cluster hosting or taglines to fool Bayesian analyzers—trace it back to your local theater or bookstore. One of the big mistakes we make as technologists is to make problems appear more difficult than they are. Success is in the storyline. Show me a person who has studied at the Actors Studio, and I'll show you someone who might elevate phishing scams to an art form.

As far as the HP pretexting scandal is concerned, common sense should have told the prosecutors that HP's general counsel would protect herself with the Fifth Amendment: it was a waste of time to subpoena her. The secret to understanding this caper lies in viewing old *Rockford Files* reruns, which is probably where the HP gashouse gang got the idea in the first place. If you really want to understand how the pretexting scam got started, subpoena James Garner.

Perception management and social engineering have been around as long as we've had wordsmiths and orators.

Here's my list of five traits that bind actors and cybercriminals together:

- They create a situation that looks plausible.
- They tailor their "performance" to a particular audience.
- They understand human nature and know how to exploit human frailties.
- They focus on one goal—getting their audience to willingly suspend belief.
- They know that they must distract their audience from thinking about the first four items on this list until after the performance/crime is completed.

Just as a phisher who sends Wells Fargo phish bait to people who have no accounts with the bank will fail, an actor dressed up like Howdy Doody will fail in presenting Hamlet's soliloquy to construction workers. And phish scams sent to digital security specialists will be no more effective than an atheist's lecture at a revival meeting.

The key to both effective acting and successful electronic crime is an understanding of an audience and the ability to "work" it. Meryl Streep, Sean Penn, Albert Gonzales, and Bernie Madoff all offered record-breaking performances. Meryl and Sean received Academy Awards, and Albert and Bernie received 20-years-to-life. All exemplary performances deserve appropriate recognition.

The next time you get phish bait in your mailbox, review it as you would a live performance, and give credit where credit's due. You might be looking at the first effort of a future cybercriminal hall of famer who'd like to be a protégé of your favorite actor.

***Hal Berghel**, Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). Contact him at hlb@berghel.net.*