THE ART OF TRICKERY: METHODS TO ESTABLISH FIRST CONTACT IN INTERNET SCAMS

ANDREAS ZINGERLE

University of Art and Design
Linz, Austria

andreas.zingerle@ufg.at

Keywords: Unsolicited Electronic Mail, Scambaiting, Computer Mediated Communication, Interactive Storytelling

Internet scammers use fictional narratives to gain the trust of potential victims. These narratives are often pre-scripted, get send out by individual scammers or scam-groups and are often copied and reused by other scam-gangs. Vigilante online communities of scam baiters try to jam the practices of these Internet scammers by using similar social engineering techniques to hook the scammers into a story and consequently interrupt their workflow. In this paper, through examples, I want to take a closer look at the scammers working methods and focus on two different strategies on how scambaiters use to approach scammers.

1. INTRODUCTION

'First contact' is a term describing the first meeting of two cultures previously unaware of one another. In this paper, I have outlined the methods by which the online communities of scammers and scambaiters craft their first contact with each other.

Today, most spam messages get send automatically over botnets, yet the so-called 419-scams[1] are still largely performed as manual labour by individuals or groups of scammers (Isacenkova, 2013). The 419-scam is so effective because it appeals to the two basic human traits of greed and superiority (Zuckoff, 2006). Falsification, impersonation, counterfeiting, forgery and fraudulent representation of facts are common tactics that scammers use to gain the trustworthiness of their victims. However, the first contact needs to be well crafted in order to be able to grab the victims' attention. After a first payment is wired, the scammer comes up with further obstacles and story plots asking for more money. This creates a vicious circle where the victim ends up paying constantly more and more money (Isacenkova, 2013).

An online vigilante group called scambaiters use social engineering techniques to get in contact with the Internet scammers. Scambaiting tactics can be seen as subversive while making use of similar strategies as scammers do. When the initial connection is made the scambaiter impersonates the potential victim as long as possible. This both to keep the scammer busy from his other criminal activities as well as to document the scam with the intention of warning others. Some use these tactics to severely criticise the scammers and to put them in the virtual pillory. There are two main techniques that scambaiters use to make this first contact with scammers: 'imposing the simple minded victim' and the 'accidentally send out email messages' (ASEM). This paper will later take a closer look at both these techniques and illustrate their main aspects with examples.

2. A SCAMMERS SCRIPTED STORYLINE

Internet scammers use a number of story lines to grab the attention of other Internet users. These narratives are mostly pre-scripted texts, which get sent out in bulk to millions of people. Freiermuth applied a rhetorical moves analysis on scam emails to assess that scripted messages follow distinctive patterns to develop a trusting relation-

1 The number *419* refers to the article of the Nigerian Criminal Code dealing with fraud.

ship with their marks (Freiermuth, 2011). Hartikainen further examines that the initial email has to provide sufficient degree of credibility and must be both convincing and compelling enough to make the mark respond. This is most often based upon a successful calibration of the narrative with the marks of superior feeling and the stereotypical understanding of Africa or Africans in general and successfully used in e.g. refugee romance scams, charity scams or war booty scams (Hartikainen, 2006). The scripted narratives get often mixed with actual on going events like the struggle of decolonization, corrupt politicians and exploitation of natural resources. This metafiction enhances the credibility of the involved characters and the whole narrative. The scammer is using the credibility of other Internet services like news agencies or other users comments to backup their story.

When a victim replies to a scam-mail, the scammer answers with yet another scripted messages further filtering the naive from the sceptical. In an ideal case the scammer can rely on his scripted narrative until he stipulates a small fee. When following a script the different tasks involved can be executed by a single independently working scammer or by a hierarchical structured gang (Interview with a Scammer, 2010). The following examples demonstrate the share of workload and responsibilities when a gang of scammers use a number of email accounts and involve several interrelated characters in the scam narrative (Hotz-Davies, 2006).

2.1. SHARE OF WORKLOAD

In the hierarchy of scammers on the lower level you find the ‘foot soldiers’ or the ‘yahoo boys’, young boys in their late teenage years who harvest email addresses and send out the initial bulk emails (Tade, 2011). Depending on the scripted story, email addresses of a certain gender, occupation or geographical locations are collected. A sign of such shared workload can be a different email address in the ‘From:’ field than the ‘Reply-to:’ field or changing locations based on email IP address analysers (Schneier, 2011). Once a victim replies to an email, the message is delivered to a different scammer.

At this level a more experienced scammer – often called ‘guyman’ – is dealing as efficiently as possible with a lot of victims at the same time. Each task demands special qualifications and has to be delegated efficiently;

an entry-level ‘yahoo boy’ does not need proper language skills when harvesting email addresses and sending initial emails out in bulks (Ogwezzy, 2012). The final money transactions are then handed over to the higher-level gang-leaders (called ‘Ogas’) who keep track of the income. This happens through an email message, where the victim is asked to contact yet another person, often claiming to be a barrister or another official representative, who will further deal with the financial transactions. The following e-mail snippet illustrates a typical example how the victim is directed to correspond with another character in this case the family lawyer James Douglas.

> *[…] I will like to inform you that every information concerning the deposited consignment is with our family lawyer Barrister James Douglas, in which case you are to contact our family lawyer who will direct you on how to take custody of the deposit […] So feel free to open up communication with him by calling him and sending your telephone numbers to him for regular communication until the deposits are transferred to you. […] Let me know as you contact the lawyer.*

Once the victim replies, the scammer at the next level of the gang hierarchy is already dealing with the victims who fully trust the story and are willing to ‘seal the deal’ by wiring the designated advance fee. According to a scammer called ‘John’, at this level one out of every 20 replies would lead to getting money out of the victim in the end (*Interview with a Scammer*, 2010).

This separation of workload facilitates the use of several interrelated characters within the narrative. The rather practical approach implies similar techniques as used in transmedia storytelling practice, making it the ideal aesthetic form for an era of collective intelligence (Jenkins, 2011). Jenkins defines collective intelligence as ‘alternative source of media power‘ that facilitates new ways for people to participate in knowledge cultures. This can be followed in the genre of fan fiction literature, as Jenkins states:

> *[…] they introduce potential plots which can not be fully told or extra details which hint at more than can be revealed. Readers, thus, have a strong incentive to continue to elaborate on these story elements, working them over through their speculations, until they take on a life of their own (Jenkins, 2011).*

3. ANTI-FRAUD STRATEGIES

There are different anti-fraud strategies that show how you can deal with a scam letter at various levels, starting from reposting the email to warn other Internet users[2] to rather sophisticated social engineering practices to engage with the scammer for a longer term (Zingerle, 2013). Each strategy requires an initial contact with the scammer. Next we will take a closer look at two methods and with the help of examples show how scambaiters intentionally get in correspondence with scammers.

3.1. STRATEGY I – THE BLUE EYED VICTIM

A popular method amongst scambaiters is to directly respond to the scammers email proposal, whether the scam-mail was found in the inbox, a spam folder or an online forum such as *Scamoftheday*.[3] No matter where the email message originates, the receiver replies to the scammers'email acting as believer of the proposed narrative and willing to engage further. A gullible reply gives the scammer the feeling of a 'fast hit', as nearly 70% of all replies wire money at least once to the scammers (Interview with a Scammer, 2010).

During the correspondence with the scammer the scambaiter further defines the created character. A scambaiter never exposes his or her real identity while exchanging messages with scammers. The scambaiter aims to conduct and starts constructing their own narrative, where unforeseen obstacles occur that can bring the scammer 'off the script'. Following actions by the scammer can be 'off-script': your questions are considered and get answered in detail; emails are answered in a rush with certain changes in sentence structure and an increase of typographic or grammatical errors (Bluth, 2010). When the scammer is 'off-script' each scambaiter has their own strategies to develop the storyline with the aim of: documenting the scam-method, collecting evidence of trust in form of photographs, audio- or video recordings jamming the workflow of the scammer and reporting bank accounts or credit cards (Zingerle, 2013).

3.1.1. EXAMPLE: 'RE: DAKAR ARTS FESTIVAL'

The 'Re: Dakar Arts Festival' project documents the practice of scammers, who announce an online open call for a fake art festival in Dakar, Senegal. The festival is just a lead story for advance-fee fraud and victims are lured

3 *http://www.scamoftheday.com/*

2 *http://www.scamwarners.com/*

into wiring money for reservations, transportation costs, commissions or other service charges without knowing that the festival does not exist. The project evolved out of open calls posted on art-forums and personal email messages that invite artists and gallerists to participate in the upcoming Dakar Arts Festival. To investigate a bit further, we started developing online characters that were in contact with the scammers. We created three virtual characters: a gallerist Peter Irrthum, an artist Heidi H. and the gallery secretary Toni Alm. The fake gallerists Peter replied to the email that the festival organizer Mariama Sy sent out:

> *Dear Dakar Arts Festival Team,*
> *my name is Peter Irrthum, I am a gallerist based in St. Gallen, Switzerland. I found your open call on absolutearts.com and find it very interesting. […] It would be really good if it is still possible to sent exhibition proposals. As you know I am a gallerist and I am always looking for international exposure for my artists and good networking possibilities for my gallery. I also think that one of my photographers would be interested to join this unique opportunity to exhibit her artwork. […] Let me know as soon as possible if it is possible to apply to the festival. Best, Peter*

This first email introduces the gallerist and his interest to participate in the festival. He even seems to be eager to get one of his represented artists to participate. After receiving a first answer from Mariama Sy, telling us more about the participation modalities, our artist Heidi H. gets in touch with them:

> *To whom it may concern,*
> *my gallerist Peter Irrthum contacted me about the opportunity to participate at your festival (Dakar Art Festival). I was immediately attracted by this offer of two reasons; I have never had the opportunity to exhibit on your continent and I have never visited Senegal. I have attached to this mail my CV. I just finished working on a photo series that could fit to your exhibition. […] What information do you need about my work? Is there a curational theme for the exhibition? Mr. Irrthum informed me as well about the offer that you benefit 50% f the travel costs. […] Please let me know if this can be arranged? Hope to here [sic] from you soon, best regards, Heidi H.*

When the correspondence with the scammers developed further, online representations like Wordpress blogs, Social Media profiles, etc., were created to backup the identities of the characters and to pursue the unfolding of the story. By cross-referencing these online representations in the correspondence we gained the trust of the scammers and this helped us collect more information about them and their practice. The collected data was reported to popular web platforms that publish open calls for artists. Furthermore, artists, state funding offices, embassies in Dakar and other art festivals were informed about the scam.

3.2. STRATEGY II — THE ACCIDENTALLY SENT EMAIL MESSAGES

A second method to contact Internet scammers is to send out 'unsolicited Bulk E-Mails', also referred to as 'accidentally sent email messages' (ASEM). Using this strategy the sender claims to have been in contact with the scammer before, apparently trusts this person, refers to a situation that happened in the past and lays out the steps how to proceed further. By instructing the scammer what to do in order to advance the cooperation the scambaiter is in control of the situation. Any scammer answering such an email steps right into the story world created by the scambaiter and is ready to follow the rules of this world.

The following example demonstrates how this strategy was tested and examining what kind of response rate engineered stories in ASEMs can have. In this example bulk emailing was used to contact scammers and receive their bank account information. The email addresses were taken from email providers blacklists and got double-checked to avoid contacting innocent people.

This was in order to report those accounts for being monitored or even closed due to criminal activities. In the email, the sender refers to a previous payment via Western Union and put in the urgent request for detailed bank account information to reduce the processing fees for the larger payment they want to make. The email is obviously addressed to the wrong person, but the scammer also sees that there is an opportunity to 'turn a fast buck' (Goffman, 2011) that is supposedly meant for someone else. The e-mail used for the test:

[…] Good that it worked out that you received the €80. I just went back to the Western Union office to send you the missing €920. […] The processing fee for sending the amount is getting quite high, if possible I want to avoid unnecessary service charges. Can you send me your bank account information? […] I await your prompt reply. Best regards a.m.

Figure 1 visualizes the response rate to this unsolicited Bulk E-Mail offer within the first five days. From the total of 500 contacted scammers, 96 emails could not be delivered due to unavailability of the email addresses. This can happen when emails get reported for fraudulent activities and therefore the account gets blocked or closed by the service provider. 404 emails were delivered to the scammers' Inboxes. Over the next five days 47 scammers (11.63%) replied, seven scammers (14.90%) replied immediately with their bank account details, 30 scammers (63.82%) wanted to pay for the processing fees, eight replies (17.03%) questioned why they were being contacted, two (4.25%) were considered insulting.

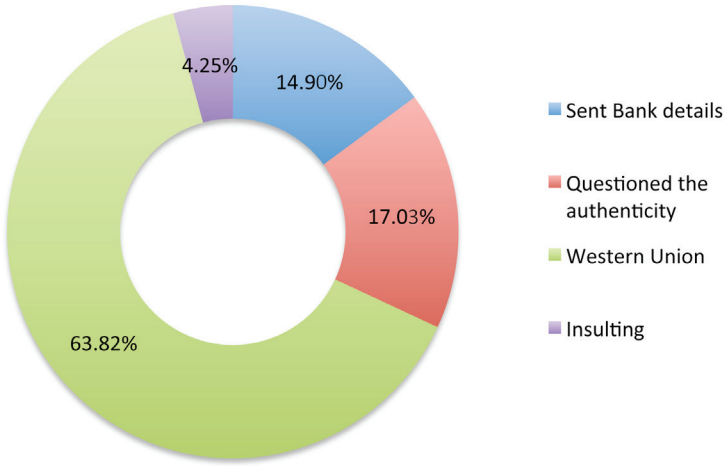

Fig. 1 Diagram of response rate

3.2.1. EXAMPLE: A RELIGIOUS GROUP EXPANDS TO WEST AFRICA

One example documented on the scambaiter forums[4] that makes use of the ASEM strategy is a transmedia story of a religious group. This online narrative makes use of a number of channels including website, several forms, ceremony manuals and audio recordings.

The bait is based on creating a church so credible and so attractive, that many scammers would want to

4 To protect the method no detailed names, links to the websites or references to the authors are listed here.

join it. Using similar language as that of an advertisement an image is created that there will be a substantial financial gain if one happened to join the church and helped it grow in countries where the group currently does not have a foothold. One of the main hooks is that the religious organization wants to expand into the West African countries and they are currently seeking local representatives to organize the congregational events. Accepted members of the church are able to receive further funds for their missionary. To be able to do this, the applicant has to fulfil several tasks: filling out membership applications, showing his dedication to the church by constructing a 'Monument of Faith' or performing and documenting an ordainment ritual.

The initial email that is sent out to the scammers is supposedly written by the secretary of the church, paving the way for the scammer to accept the story and become a member of the church:

> *Our church states that we can only do business with other members. [...] there may be a great many opportunities to do something together, including helping you with your affairs. [...] Best regards,*

In the case that a scammer answers to the email, they receive an answer yet from a new character 'Director of Membership' of the church:

> *[...] There are only a few steps need to be taken to become a member. Have you had a chance to visit our website? If not, I suggest you do to become acquainted with our church. I am looking forward to hearing from you soon!*

He refers to the secretary who forwarded him the email and refers to a detailed website of the church as a source for further information about the religious movement. A phone number is provided that is linked to a mailbox where one can listen to recent church activities and follow upcoming event schedules. If a scammer is still interested to continue with the acceptance process, a member request application is sent to him. This pdf includes a personal letter of the reverend, a five pages long survey that the applicant has to fill out. Additionally several photographs of him and other potential

church members in various defined poses have to be taken and attached.

Once the scammer sends back all this material it gets revised and a membership status approved. The scammer is further asked to build a physical sculpture to prove his faith in the religious group and all involved participants. A pdf file illustrates the parameters to build a sandbag-pyramid with 4x4 meters width at the base and a height of about three meters. Once the pyramid is successfully built the requested photo documentation is sent to the reverend, an additional 'ordainment ceremony' has to be performed and documented. The ceremony asks one participant to dress up as a reverend in white long dress, light a torch, recite gospel texts and perform a ritual including other participants who carry him around the pyramid.

If the scammer has gone through the ritual, one of the authors states:

> *Your lad is now ready for anything. You own him. At this point, he has totally devoted himself. […] You will be able to ask him to do anything, and he will do it.*

This example uses ASEM in combination with transmedia story telling in a successful way for the scambaiters. It demonstrates how well these strategies can be used. However, the efficiency and ethical aspects of these strategies pose valid questions. From this stage onwards the authors of the scambait suggest to continue with a 'safari', a practice to get the scammer away from his computer and travel to a remote place (Zingerle, 2013). The authors have also felt a rising need to comment on their strategies as well implying that a discussion around the ethics of the scambait is essential as well. The instructions end with an ethical note on the methodology:

> *These ethical dilemmas are easy to deal with. If you don't feel comfortable making a fool out of a lad who thinks that he is truly doing something good, then just stop. […] Quit baiting and go do something else.*

Scammers contact their victims by using the ASEM method, like in this example where the subject line starts with a 'Re:' that indicates a former contact between the parties and the sender refers to an already wired payment:

[...] I am contacting you because I've sent you the first payment of $5,000 today from your winning funds total amount of $1.5Million USD. Therefore you need to contact western union agent Mr. Tony Masinas, for him to give you the transfer payment information and MTCN. [...] Do get in touch with me once you have received the transfer. Best regards.

3. CONCLUSIONS

This paper has given an account of the different strategies both scammers and scambaiters use to get in contact with their potential victims. Scammers use pre-scripted narratives to get in contact with people. Scambaiters on the other hand pose as the 'blue eyed victim' when replying to a scammers email to gain the trust of the scammers and try to bring the scammer 'off-script'. Another method to contact scammers is the 'accidentally sent email messages' (ASEM) in bulk method. Both strategies influence the way of storytelling: the 'blue eyed victim' method lets the scammer tell the scripted narrative and the scambaiter slowly infiltrates or tries to infiltrate it whereas within the 'ASEM' strategy the hooked scammer is compelled to play along the scambaiters narrative from the very beginning. In both the examples we have seen that scambaiters use transmedia storytelling practices and spread their story over different social media channels. By doing so scambaiters can reference to this websites in their correspondence with the scammer, unfolding multilayered stories where several twists and turns are possible. Individuals or several scambaiters who work together can operate with both strategies.With both methods it was possible to collect information about the scammer and warn potential victims. Some cases led to the arrest of the scammer (GNA, 2006).

Where law enforcement has failed to internationally develop effective ways to take action against the global phenomena of online scams the vigilante online communities of scambaiters act as a global civil movement against Internet fraudsters. They document the scammers practices, warn potential victims and report to hosting providers, webmail services or law enforcement. However, moral and ethical discussions arise when scambaiters humiliate their counterparts. While scambaiters come from diverse backgrounds and are

motivated by various reasons (Zingerle, 2013) ‘ethical’ approaches to scambaiting are continuously under discussion in scambaiting forums. Whereas it is generally agreed, that what differs a scambaiter from a scammer is that a scambaiter does not seek for financial gain, there are a number of documented cases where scambaiters do not agree on the morals of the scambait. These are cases like the ASEM method described in 3.2, or other scambaits where scammers were sent on long lasting and sometimes dangerous travels or were getting tattoos with the logo of the church, which resembles an act of physical punishment. An important and interesting topic for further research would be to examine various guidelines on safe and ethical communication with scammers that emerge from the discussions in the scambaiter forums.

REFERENCES

Berry, Michael. *Greetings in Jesus name! The scambaiter letters.* York: Harbour, 2006.

Bluth, Banana. *Area 419: Scambaiting Radio*, Episode 3. Retrieved Apr. 6, 2014 from http://itunes.apple.com/us/podcast/area-419-scambaiting-radio/id359035187, 2010.

Brunton, Finn. *Spam: Shadow History of the Internet.* The MIT Press, 2013.

FTC. Federal Trade Commission Consumer Information, *Fake checks*, Retrieved Apr. 6, 2014 from http://www.consumer.ftc.gov/articles/0159-fake-checks, 2012.

Freiermuth, Mark. *'This Transaction Is 100% Risk-Free!' Why Do People Fall Prey to E-Mail Scams?* LANCOMM – Int. Conference on Language and Communication 2011.

GNA. *Three computer frausters arrested*, Available online: http://www.ghanaweb.com/GhanaHomePage/crime/artikel.php?ID=106927, 2006.

Goffman, Erving. *Self Claims: On Cooling the Mark Out: Some Aspects of Adaption to Failure.* In The Goffman Reader, edited by Lemert, C. and Branaman, A. Malden: BlackwellPublishing, 1997.

Hartikainen, Elina. *The Nigerian Scam: easy money on the Internet, but for whom?* Michicagoan Graduate Student Linguistic Anthropology Conference, 2006.

History of 419 Spam – Spam Mails, Advance Fee Fraud, Spammers, Spam Victims. Retrieved Apr. 6, 2014 from http://www.nigerianspam.com/history-419-scam.htm

Hotz-Davies, Ingrid, and Anton Kirchhofer. *Internet fictions*. Newcastle upon Tyne: Cambridge Scholars, (2009).

Interview with a Scammer. Retrieved Feb. 14, 2013 from http://www.scamdetectives. co.uk/blog/2010/01/26/interview-with-a-scammer-parttwo/, 2010.

Isacenkova, Jelena, Olivier Thonnard, *et al.* *Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations.* IEEE Security and Privacy Workshops, pp.143-150, Retrieved Apr. 6, 2014 from http://www.ieee-security.org/TC/SPW2013/papers/data/5017a143.pdf, 2013.

Jenkins, Henry. *Transmedia Storytelling 101.* Retrieved Apr. 6, 2014, from http://henryjenkins.org/2007/03/transmedia_storytelling_101.html, 2007.

Krebs, Brian. *Online Service Offers Bank Robbers for Hire.* Retrieved Apr. 6, 2014 from http://krebsonsecurity.com/tag/money-mules/, 2012.

Ogwezzy, Michael. *Cybercrime and the profileration of Yahoo addicts in Nigeria.* International Journal of Juridical Sciences, ISSN 1843-570X, nº. 1 (2012), pp. 86-102.

Schneier, Bruce. *Interview with a Nigerian Internet Scammer.* Retrieved Apr. 6, 2014 from https://www.schneier.com/blog/archives/2010/02/interview_with_16.html , 2011.

Tade, Oludayo, and Ibrahim Aliyu. *Social Organization of Internet Fraud among University Undergraduates in Nigeria.* International Journal of Cyber Criminology, vol. 5, nº. 2, pp. 860–875, 2011.

Zingerle, Andreas, and Linda Kronman. *Humiliating entertainment or social activism? Analysing scambaiting strategies against online advance fee fraud.* Cyberworlds 2013 Conference, DOI: 10.1109/CW.2013.49, 2013.

Zuckoff, Mitchell. *The Perfect Mark*, The New Yorker: PRINTABLES 2006-05-08, 2006.