Towards a categorization of scambaiting strategies against online advance fee fraud

Andreas Zingerle, M.A.
University of Art and Design, Linz, Austria

ABSTRACT

Scambaiters are individuals in online information communities specializing in identifying, documenting and reporting actions of so-called ’419 scammers’. A qualitative research approach was applied to two active scambaiting communities - 419eater.com and thescambaiter.com. Content analysis of several discussions and the examination of interviews from the web radio ’Area 419: Scambaiting Radio’ resulted in the seven categories of scambaiting techniques that are presented in this article. The aim is to both give a wider understanding of the scope of existing Internet scams as well as answering questions of why and how individuals or communities of scambaiters take action against Internet scammers. The analysis on various scambaiting practices is intended as a base for future discussions, for instance, whether some scambaiting methods should be implemented in media competence training.

Keywords: Unsolicited electronic mail, 419 scam, Computer mediated communication, Online Communities.

INTRODUCTION

We all receive them in our Inboxes - unsolicited emails with mass advertisements offering cheap electronics, medicines without prescriptions or phishing mails asking us to update our banking information. Sometimes, a once in a lifetime opportunity slips through the spam filter, revealing a story and offering us a ’get rich quick’ opportunity by just paying a little amount of money upfront. Once the receiver detects a scam email, it is either deleted or spam settings get adjusted. Some recipients, perhaps out of frustration or misinterpretation, take the time to reply to the scammer with messages like ”*unsubscribe*” or ”*please take me off your list*”. Cybercrime is a growing phenomenon in the interpersonal interactions of computer-mediated communications. In 2012 the Internet Complaint Center (IC3) received over 290,000 complaints; reported dollar loss was over 525 million (Internet Complaint Center, 2013). In the past victims were mainly contacted by ’unsolicited bulk emails’: now, the widespread use of social networking services (SNS) has made it easier for scammers to contact potential victims. The general tactics of advance fee fraud can be traced back to the early 16th century. Face-to-face persuasion known as the Spanish prisoner scheme was widely used to trick victims. Over centuries the basic scheme has been adapted to new ways of communication: letters, telegraph, fax, phone or Internet. A global boost happened in the 80’s, with the growing use of emails, enabling scammers to contact a large number of people fast and very cost efficiently (Brunton, 2012). In these emails the recipients’ identity and the context of the message is irrelevant as long as the message is applicable to a large number of potential victims. According to the 2011 report of the Messaging Anti-Abuse Working Group, 88-90% of email traffic is considered ’abusive’ letters that are

unwanted or unexpected, or those trying to exploit the recipient (Messaging Anti-Abuse Working Group, 2011). These schemes are also known as ’419 scams’, referring to the article of the Nigerian Criminal Code dealing with fraud (Brunton, 2013). Scammers use different story-scripts to persuade their victims to pay money upfront. An efficient script seduces the victim into a fast initial payment and allows a constant flow of further payments until the victim is either bankrupt or loses trust in the scammer. After a successful scam the scammer often re-activates a victim, usually with a follow up scheme like contacting the target in a new role by posing as law enforcement.
Scambaiting arose as a counterattack to ’419 scams’. This online vigilante community of scambaiters investigates scam emails and implements social engineering techniques to document, report or warn potential victims. Scambaiters have own personal motivations to justify their actions. As Tuovinen et al. point out, these motives can range from community service and status elevation to revenge for being a victim of a similar scam in the past (Tuovinen, 2007). Through the documentation and sharing of these plots, scambaiters waste the scammers’ time, exploit their resources and raise awareness about online fraud.

SCAMBAITING STRATEGIES

There are two main motives for writing this paper. One is to summarize and document seemingly endless threads from scambaiter forums. This is mainly because information from these forums can easily disappear like in September 2012 during the merge of thescambaiter.com with scamtacular.com. A second reason is to emphasize that there are scambaiting methods that can be seen as ’antifraud activism’ rather than humiliating status elevation. The humiliating methods that do exist among scambaiters are documented by Krings (Renner, Ryan, Hoff, & Krings, 2013). Yet, by analyzing the ’Area 419: Scambaiting Radio’ (Bluth, 2010), forums like 419eater.org and thescambaiter.com, it is clear that there are also ethical codes among scambaiters and these communities are developing several social engineering tactics to hinder criminal activities, warn victims and raise awareness about continuously evolving scam techniques. By dividing scambaiter activities in the following seven categories, and by giving some examples of how each category practices scambaiting, we realize that scambaiting is far more diverse than just humiliating the other. The following list of characteristics shows trends of how scambaiters think actions and responses against scammers are needed.

The Scam Alerters

’Alerters’ identify and report online scams in order to increase general awareness of Internet scams. They warn individuals and groups who are vulnerable to scams by providing detailed and reliable information. Furthermore, they supervise victims to protect them against follow-up scam attacks. There are several websites and forums that provide information for potential victims; romancescam.com spotlights particular issues like online dating scams, whereas others like scamvictimsunited.com provide support for fraud victims. By taking a closer look at scamwarners.com, we see that members of 419eater.com initiated the website to document unsolicited emails and fraudulent offerings. The forum serves as a platform to authenticate and discuss received emails. As a result, other potential victims are informed about new scam types and warned against email proposals that are just ’too good to be true’. For victims who have fallen for a scam before, this platform provides a section with FAQs and further advice.

A ‘big order’ from China

In the following example a skeptical person named ‘zawilec’ posts a business proposal that one of his clients received. He is sure that people try to scam his business partner, still he seeks for an ‘expert’s opinion’ regarding the proposal. Attached to the message is the email with the offer, stating an import and export company who is trading environmental equipment and want to purchase a batch of Aluminum pieces. They also list their phone number and company website[1].

"Dear Sirs,
We are an international trading company in Xi an China, specialized in importing and exporting, which mainly involves in environmental equipments, chemical equipments, construction equipments and machine parts. Because of the needs of our clients, we are going to purchase a batch of Aluminum Pieces. If necessary, we will send the drawings of the products to you by attachment. If you can produce or have similar products like this, please quote us with the price of FOB or CIF, and then we can expand further steps in our cooperation. […]

A scam warner member by the name ‘AlanJones’ analyzed the DNS entries of the companies website and figured out that the site was setup in September 2013 despite they were claiming to be in existence since 1998. Instead of using the official Top-level Domains email address they were using a free email service[2].

The skeptical poster ‘zawilec’ continued his search and posted:

I dig up a little bit more and it seems like it's classic example of "big order scam", otherwise known "china scam". Amazing how far some scammers can go. Disgusting but I'm impressed.

The user ‘TerranceBoyce’ wrote on Nov 29, 2013:
“[…] companies don't place orders without initial negotiations, bargaining and discussions. The intention is that common sense is overlooked in the seller's eagerness to secure a lucrative deal. Chinese companies speak Chinese and would have their website written in Chinese but it supports a scam directed at the rest of the world, not the Chinese market.”

The user ‘Rainbow76’ wrote on Dec 2, 2013:
This company doesn’t exist in China! It is scam; it is called "guilin" scam, which running for years, google it, you will find more!

The last entry in this thread is by ‘Shoggsy’ on Dec 07, 2013:
“Client received a similar email from the Xi an Xian Dong People. […] My client flew there, had dinner twice with the company people including a mandarin translator but had to foot the bill both times. They also asked for 'notary' fees up front -and gave a personal bank account with the line ‘It's easier to put in personal account than company account'

---

[1] http://chinaxiangdong.com/

[2] http://www.163.com/

FYI - no legitimate Chinese businesses ever ask for 'notary' fees or to fly to China to sign a contract for a large amount of goods, sight unseen. Stay well away!"

The Trophy Hunters

'Trophy Hunters' are scambaiters who reply to scam emails, being fully aware that the emails are written by scammers. Scambaiting involves tricking Internet scammers into believing you are a potential victim. This means that scambaiters turn the tables on the scammers and lure them into incredible story-plots, constantly baiting the fraudsters who hope to receive a lot of money. These type of scambaiters aim for so called 'trophies'. A trophy - something that the scambaiter acquires from the scammer - can be of physical or virtual nature. It functions as proof of a scammer believing the story-plot and is an evidence of additional work or expenses that were caused while following the terms of the scambaiter. A trophy can vary depending on the actual goal of the scambaiter: it can be some kind of documentation like a photo, recorded audio or video, a filled out form, a fake bank check, sometimes even hand crafted objects (Berry, 2006). A trophy can also be acquired when the scambaiter manages to lure the scammer into fulfilling a time consuming and tedious task to interrupt the scammer's workflow. Sometimes the task can involve geographical relocation or cause personal loss of resources in the form of money payments. Some scambaiters either take this to the level of emotional punishment by finding methods to humiliate scammers or to the level of physical punishment by making the scammer get a tattoo. Trophies are often collected in special sections of a scambaiting forum called 'Hall of Shame[3]' or 'Mugu Museum[4]'.

There are many different examples of trophies, ranging from humiliating photographs to documents that show the scammer's wasted time, unveil their working practice or help to identify the criminals who run the scam. Also the way these trophies are documented can vary from photographs to audio or video recordings, handwritten forms or even sculpted objects.

Wasting their time: The story of the 'incredible shrinking artwork'

A creative approach comes from the trophy hunter 'Mike Berry' who published his story 'The incredible shrinking artwork' in the book 'Greetings in Jesus name' (Berry, 2006). He impersonates the art dealer 'Derek Trotter' who runs the company 'Derek Trotter Fine Arts & Artists Scholarships'. He is interested to either present upcoming artist's in one of his galleries or give scholarship donations ranging between $25,000 and $50,000 to potential art students.

The author sends this email proposal as a reply to scam emails he receives. Once a scammer shows interest, 'Derek Trotter' sends detail documents of how to prove the artistic talent in order to receive some scholarship. It includes the creation and submission of a wood carved object according to a set of provided photographs. In a first example he sent out a small object from the UK series 'Creature Comforts'. After the submission of the carved object, some twists in the plots were taken to make the scammer carve an object and submit it again. This kept the scammer wasting more time to craft and send another object, this time a Commodore 64 keyboard.

---

[3] http://forum.419eater.com/forum/album.php/

[4] http://www.thescambaiter.com/photopost/

Documenting their practice: The 'Re: Dakar Arts Festival'

The 'Re:Dakar Arts Festival' project documents a scammers attempt to organize a fake art festival in Dakar, Senegal. By copying the well-known Dak'art biennale, the fraudsters invite gallerists and artists to participate in the upcoming 'Dakar Arts Festival' (now 'Dakar International Festival of Visual Art' (I.C.V ARTS)). The transmedia story follows the characters of a gallerist, an artist and a secretary who are in contact with the festival organizers to participate in the upcoming exhibition. The story is told in an interactive installation and online through social media channels. Each character maintains online blogs and social media profiles where they tell their personal perspective of the story. Depending on time and interest the reader can choose which storyline to follow and when to dig deeper into the narrative. The outcome of the one-month correspondence in addition with further information about the scammers practice could be visualized in a flow diagram (see Figure 1). The various online traces, a website[5] and the art installation inform about the scammers practice and question the trust we put in online representations.

Figure 1. Anatomy of the 'Dakar Arts Festival' scammers practice

The Website Reporters

In order to appear professional and to increase their trustworthiness, Internet scammers often run fake websites on Top Level Domains (TLDs) as part of their scams. These websites mimic real businesses - online shops, banks, charity organizations, religious groups or IT companies. 'Website Reporters' identify these websites for instance by linking DNS entries to scammer databases. They then document any illegal activities and report their findings to the hosting provider to get the websites removed or banned. The largest Internet community dedicated to stopping these activities is called 'Artist against 419' (AA419[6]), which hosts one of the world's largest databases of fraudulent websites. Once a fake website is registered, AA419 informs the hosting provider of the site, giving detailed evidence of illegal activities and requesting the site to be shut down for violation of terms of business. In 2003, the group started using custom software like Muguito or Lad Vampire to organize virtual Flash Mobs. The programs repeatedly downloaded images from the fraudulent website until the bandwidth limit was exceeded. This action can be considered as 'bandwidth hogging' rather than a Distributed Denial-of-service attack (DDoS), since a DDoS attack targets the whole server and not just a single website. The group provoked a lot of discussions and controversy with these illegal virtual Flash Mobs, but the group itself saw this as a valid way to take action against hosting providers that did not react to their requests to take down a fraudulent website. According to their website, the group stopped organizing virtual Flash Mobs and discontinued the development of those particular software programs after September 14th, 2007. In the same year, AA419 teamed up with the London Area Metropolitan Police fraud alert unit. They also continued maintaining good relationships with many hosting providers, who now use the AA419 database to locate illegal sites and delete them from their servers (Espiner, 2007).

[5] http://www.dakarartsfestival.net/

[6] http://www.aa419.org/

The Bank Guards

Some scambaiters specialize in obtaining background information on all kinds of bank related issues like overpaid check validation, phishing sites, money mules, reporting fake banks or closing bank accounts.
'Bank Guards' often target scammers who use bank accounts in their payment procedures, e.g. charity scams. By reporting bank accounts, 'Bank Guards' believe that scammers lose money in a legitimate manner or other victims who act as 'money mules' are warned.

Scammers use different tools and techniques to divulge personal financial information from their victims: credit card numbers, account username/passwords, social security numbers, etc. Personal documents like passports or birth certificates and (electronic) signatures can be collected. A scammer can use this information for Identity fraud: starting businesses in the victims name, open accounts, gaining trust or other benefits in that person's name.
Scambaiters try to document and monitor this fraud attempts.

Community driven reporting game

Within the scambaiting community, collecting and reporting fake bank accounts can become a game itself, where the challenge is to gather as many accounts as possible within a certain timeframe. Extra points were given to talented activists who were able to get more than one account information from the same scammer. A special focus was given to fraudsters who run Coca-Cola lottery scams, their bank accounts scored double. To motivate the participants, the winner received a 'Premium Membership' of the 419eater forum to access additional content. The challenge was open for two months and the participating bank guards could report over 160 bank accounts.
The sharing of the story plots and tactics with the community results in new efficient methods to counterattack this kind of scammers' practice. By documenting and reporting criminal activities to bank officials, they monitor account transactions, freeze accounts and inform local law enforcement.

The Romance Scam Seekers

People increasingly use 'Social Networking Sites' (SNS) to keep in touch with friends or find new ones to extend their network. Some use SNS, chat rooms or special 'Online Dating' websites to develop a personal, romantic, or sexual relationship with like-minded people. Scammers use these sites to set up their fake profiles, often targeting single men and women who are willing to pay them money. These profiles often use photos taken from modeling or social networking sites, making the photographed people as much victims as the people who take them as legit. This sort of online relationship can be a very intense experience, since scammers will try to get in touch with the victims on a daily basis by using multiple media channels (Email, Chat, VoIP, etc.) as well as send physical evidence to acknowledge their deepest love. Blinded by love, victims pay upfront for translation fees, medical bills or visa fees. 'Romance scam seekers' are fully aware that scammers contact victims with the intention of tricking them into making fraudulent payments. They pretend to be flattered by the scammers' attentions and give the impression that they can be trusted easily. These scambaiters then document the scammers' practices and post their findings on victim warning forums like scamdigger.com or compile stories for booklets like 'Hello Sweaty' (Cambaiter, 2012). They also try to track down the

person whose photos are used in the scam and block the scammer from creating more fake profiles on dating websites.

A romancescam.com forum member named ‘sandstone’ posted a concern[7] about her close friend; let’s call her Mary, who is romantically involved with a man she met on Facebook. Since Mary is currently going through her divorce she is vulnerable to trust strangers. The man claims to be a CIA investigator living in Michigan, USA. He inherited a large sum of money and wants to help Mary to buy herself a new home. Mary was also in contact with other female friends of her new crush who all seemed legit and told her a similar story. This made Mary believe and trust the guy. They chat, text and send pictures back and forth every day. The friend ‘sandstone’ is very concerned because the whole story sounds just ‘too good to be true’. She tried to search online for the name and phone number to find evidence that the guy is a fraudster. She asks for help to convince her friend Mary to be more cautious with her crush.
Different forum moderators and admins tried to find evidence to the authenticity of the CIA investigator. The forum members agreed that it sounds like a scam but would also need more detailed information to further investigate the person. One suggestion was that Mary should accept the offered money and that ‘sandstone’ as a close friend should be alert about the transaction process. If Mary receives a cashier’s check she should call the bank that drafted it to verify the funds. If it is a scammer, the check will be forged and Mary can hardly deny the truth. Besides that, forum members gave security tips how-to deal with personal financial information.
The last message in the thread is written six weeks later where another person fell victim to a similar romance scam. She actually transferred money to the fraudster and found out too late that the person who claims to love her is actually a scam attempt. She could file a report at the police who arrested a linked accomplice.

In case of romance scams it is important to understand that dating cultures are diverse and each individual asking or providing financial help is not necessarily a scammer. As Jenna Burrell describes in her book ’The invisible Users’ Africans in general face prejudices (because of West African scammers) when trying to get in contact with strangers online. Several West African countries are blacklisted and access to Online Dating, Internet Banking or Auction Sites is blocked. Denied access to information and services based on geographical location reveals the unequal and undemocratic side of the Internet (Burrell, 2012).

The Safari Agents

’Safari agents’ are scambaiters who try to persuade the scammers into leaving their working space, so it becomes physically impossible to continue the illegal activities. As a guideline, scambaiters either try to encourage scammers to travel a minimum distance of 200 miles or cross the border into a neighboring country. This way, the scammer is kept busy with harsh travel conditions and cannot keep up with the daily work. The scambaiters often ask for various ’trophies’, trace back the emails IP-addresses or utilizes other web services to confirm actual travel as a successful safari.

[7] http://romancescam.com/forum/viewtopic.php?f=22&t=66217

Two scammers missing - The Road to Chad/Dafur

In May 2006 a well-documented safari ended with two scammers being sent from Lagos, Nigeria, to the violent and desolate Chad-Sudan border. Once there, they were to meet a rich reverent who promised them their funds and additional compensation for their exhausting travel. The scammers were in contact with the scambaiter several times after leaving Lagos. They crossed the border into Sudan and went missing.
The following email snippets outline the correspondence of the three scammers, two who travel to Sudan and one who stayed in Nigeria with the scam baiter who imposed to be a reverent. This is the last message that the scam baiter received from one of the two fraudsters:
From Fredrick Okonji Sun May 14, 2006:
"Our boss has instructed me to write to you. I am sorry to tell you Mr. Williams is sick from all the travel. We need rest. […] I have fear about the security in the area you are in. I spoke to a man that said the area was highly in secured and that I have to be very sure of where I was going. […] Thanks, Fredrick Okonji"

Days later the correspondence continues with a so-called 'Barrister Koffi Kuku' who is located in Nigeria:
From koffi kuku Sat May 20, 2006
"I received the news from Sudan that the boys are in jail in Khartoum the capital of Sudan. The police say they can not talk on the phone until august. They are being exploited by bastard police who is very wicked and says the boys are terrorists. […] Getting to Sudan is difficult for me because of many regulations in Nigeria. May God continue to be with us. Barrister Koffi Kuku (Esq)."

By tracking the barristers Email IP address it seemed that he had travelled to Khartoum to get his fellows released. After going to the Kober prison and talking to officials there he found out that the story of his imprisoned fellows is untrue. Still their whereabouts remains unknown:
From koffi kuku Fri May 26, 2006
"Smart guy, the officials that I talk to say that your church does not exist anywhere and is not at any camp in chad. […] I can see now that you are a fraud playing serious games. What do you gain with this? […] i will spend my life to find you and when I do you and your family will suffer terrible as i have, I promise."

This documentation provoked several discussions within the community about scambaiting ethics. The involvement of 'innocent third parties' and the fact that the scammers stranded in a conflict zone brought some baiters to call this safari an unmoral act. In a statement released on the documentation website, the scambaiter tries to explain his actions:
[…] if you read this bait carefully, you will see that they intend to steal everything they can, no matter who it was from. In this case, the scammers know full well that they are stealing from a priest who is using this money to save the lives of Sudanese families fleeing Darfur. So, am I going to lose any sleep if these guys find themselves in danger? No. Not for a second.

[…] Baiters like me have sort of an unwritten rule about not involving innocent third parties when baiting. The idea is that we do not pretend to be a real person that can be found by a scammer and thus, put this real person at risk. Some baiters have taken this ideal way too far in my opinion. In this particular bait, two of the scammers come in contact with UN security

personal near some of the refugee camps in Eastern Chad. This helped verify the scammers' locations. Some baiters claim that this contact broke the 3rd party rule.

[…] I have heard people claim that the baiter would be responsible if the criminal being baited was hurt during the bait. […] The scammers knew well in advance that they were traveling into a dangerous region but chose to do it anyhow. And once again, what was their intention? To steal money from some of the neediest people on earth. […] Let me also point out that there is no evidence that anyone was killed or hurt in this bait.

To support the 'Safari agents' trustworthiness, a scambaiter created a website to mimic a hotel business that offers their services to travellers in the region. It serves as an example of how detailed the story worlds of scam baits can evolve. This website claims to represent a small, family run business with a chain of Budget Hotels in West Africa. Fellow scambaiters can use the website to trick the scammer into believing that their character has booked a stay there and wants to meet the scammer at the hotel. The website offers a registration desk, where the scammer can confirm the victims booking. In this example, the Hotel website serves as additional bait to ensnare the scammer and make him believe that the victim has indeed traveled to Africa.

The Inbox Divers

'Inbox Divers' are social engineers who log into the scammers email account and warn potential victims or report ongoing criminal activities. Browsing through an email Inbox gives a very personal insight into the working methods of a scammer. Scammers often use email inboxes to store additional information, like other account passwords, documents they use to gain victims trust, email-drafts unveiling their scamming practice or chat-conversations with fellow gang members. Since September 2009, a scambaiter has been collecting email accounts and potential passwords of scammers and provides them to his fellow scambaiters. These scambaiters then log into the scammers email account to monitor their practices.

Analyzing a scammers correspondence

In June 2012 I received an email where the US Ambassador of the Benin Republic reached out to his fellow Americans to seek for assistance in a business proposal. Attracted by his explanations on trust and reliance I replied to see how the story develops.

Without mincing words, I am convinced 100% that you have had bitter experience with various 'scam claiming to be high government officials and thereby defrauding you of your 'hard-earned money'. […] I was on a Foreign Mission here in Benin as a US Ambassador. […] I do trust you and I expect you to show me the same trust and respect in return since trust is a 2-way street. On the other hand, trust is a relationship of reliance. Trust also means being able to predict what other people will do and what situations will occur. [...]
Trust is both an emotional and logical act. Emotionally, it is where you expose your vulnerabilities to people, but believing they will not take advantage of your openness. Logically, it is where you have assessed the probabilities of gain and loss, calculating expected utility based on hard performance data, and concluded that the person in question will behave in a predictable manner. In practice, trust is a bit of both. I trust you because I have experienced

your trustworthiness by merely believing in what I have said, even when you have not seen me, and because I have faith in human nature. [...]
Frankly speaking, I understand that anyone in your shoes will feel betrayed, but I still want you to show me your trust by giving me the benefit of doubt on this delivery arrangement. My identity and personality is verifiable, and I promise to deliver the consignment to you in the United States without any hitch. [...]
I will use my position and personality to deposit the $3.700,000,00 USD into your bank account in the United States without questioning from the financial monitoring authorities, since all documentations proving the legitimacy of the funds has been processed. […] You can send it via western union Or Money Gram with below name. [...]

After some email exchange I had the chance to access the scammers webmail account. From that moment on I could monitor the email traffic and see how active the scammer was using the account.
Between July 8th and November 11th 2012, around 324 Emails were received. By analyzing the body text and the attachments of each email about 113 emails are considered trustful victims, at least seven people paid money to the scammer. About 20 people could be warned 'in time' so they stopped the payment procedure. Around 183 emails were considered insulting. By warning everyone who seemed interested in the proposal the scammer then changed the story script. As this change didn't bring him better revenue, he finally gave up the account.

CONCLUSIONS AND OUTLOOK

In this article I have presented individual or community driven scambaiting strategies to take action against Internet scammers. A lot of time and effort is used to document and share the methods of scammers to warn other Internet users. Figure 2. illustrates the different scam baiting strategies and shows them in relation of legality, humiliation and social activism. 'Scam Alerters' or 'Romance Scam Seekers' post scam emails and give tips to victims on how to avoid further scamming schemes. 'Website reporters' compile a register of fake websites and cooperate with hosting providers to get the websites shut down. 'Bank Guards' report the scammers bank accounts to officials or take fake checks out of circulation. 'Inbox Divers' infiltrate scammers email accounts to warn victims and document organized scamming activities.

Figure 2. Diagram of scambaiting strategies

On the other hand there are also scambaiting methods that are motivated by finding ways to humiliate or even punish the scammer. In this category are: 'Safari Agents' who lure scammers into leaving their computers and traveling to remote areas. The main motive is to jam scamming workflows. However, the scammers often end up getting stranded in remote areas where they face dangerous situations. Some 'Trophy Hunters' use humiliating methods like asking the scammer to send embarrassing photos, others try to document their practice or waste their time. The scambaiter community questions these methods and extreme cases prompt discussions about scambaiting ethics. In future research, I plan to test whether some legal scambaiting tactics have educational potential, which can be used for 'anti-fraud activism'. Based on scambaiting methods presented and analyzed in this paper we developed a workshop and a booklet called

‘419-fiction - anti-fraud activism’ (Zingerle, Kronman, 2013). The aim is to present various online scams, give tips on how to identify them, introduce security strategies to safely navigate the Internet, question the trustworthiness of unknown online contacts and discuss ethical and moral issues of scamming and scambaiting. The workshop together with the toolkit combines story driven plot lines with social activism. The idea is to bring forth scambaiting as anti-fraud activism promoting the cause to document scams and warn potential victims in ways that are creative but not humiliating or illegal.

REFERENCES

Berry, M. (2006). Greetings in Jesus Name. Harbour Books.

Bluth, B. (2010, Oct. 24). Area 419: Scambaiting Radio. Retrieved from http://itunes.apple.com/us/podcast/area-419-scambaiting-radio/id359035187

Brunton, F. (2013). Spam: a shadow history of the Internet.

Burrell, J. (2012). Invisible Users: Youth in the Internet Cafés of Urban Ghana. The MIT Press.

Cambaiter, W. S. (2012). Hello Sweaty. CreateSpace.

Espiner, T. (2007, Jan 17). Police maintain uneasy relations with cybervigilantes - CNET News. Retrieved Dec 18, 2013, from http://news.cnet.com/Police-maintain-uneasy-relations-with-cybervigilantes/2100-7348_3-6150817.html

Internet Complaint Center. (2013, May 14). IC3 Annual Report 2012. Retrieved Dec 18, 2013, from http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf

Messaging Anti-Abuse Working Group. (2011). Retrieved Dec 18, 2013, from http://www.maawg.org/

Renner, K. N., Hoff, D., & Krings, M. (Eds.). (2013). Medien. Erzählen. Gesellschaft.: Transmediales Erzählen im Zeitalter der Medienkonvergenz (Vol. 2). Walter de Gruyter.

The Road to Chad/Darfur. (2010). Retrieved Dec 18, 2013, from http://www.419eater.com/html/RoadToChadDarfur/

Tuovinen, L., Röning, J., Tuovinen, L., & Röning, J. (2007). Baits and beatings: vigilante justice in virtual communities. In Proceedings of CEPE 2007. The 7th International Conference of Computer Ethics: Philosophical Enquiry (pp. 397–405).

Zingerle, A., & Kronman, L. (2011). Transmedia Storytelling and Online Representations-Issues of Trust on the Internet. In Cyberworlds (CW), 2011 International Conference on (pp. 144-151). IEEE.

Zingerle, A., & Kronman, L. (2013). 419fiction - anti-fraud activism. Retrieved Dec 18, 2013, from http://419fiction.kairus.org/