Humiliating Entertainment Or Social Activism?

Analyzing Scambaiting Strategies Against Online Advance Fee Fraud

Andreas Zingerle, M.A.
University of Art and Design,
Linz, Austria
andreas.zingerle@ufg.ac.at

Linda Kronman, M.A.
Kairus.org
Linz, Austria
linda@kairus.org

Abstract— **Cybercrime is a growing phenomenon within the interpersonal interactions of computer-mediated communications. In 2012, the Internet Complaint Center (IC3) received over 310,000 complaints; reported dollar loss was over $480 million. In the past, victims mainly got contacted by unsolicited bulk emails (UBE); now the widespread use of social networking services (SNS) has made it easier for scammers to contact potential victims – those who seek various online opportunities in the form of sales and rentals, dating, booking holidays, jobs, etc.**

Scambaiters are online information communities specializing in identifying; documenting and reporting actions of so called '419 scammers'. A qualitative research approach was applied to the 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" resulted in the seven categories of scambaiting techniques that are presented in this paper.

This paper aims to give a wider understanding of both 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 presented analysis on various scambaiting practices is intended as a base for future discussions, for instance, whether some scambaiting methods can be included in media competence training.

Keywords- 419 Scam, Scambaiter community, Computer Mediated Communication (CMC), trust, online representation, Media competence training

I. INTRODUCTION

General tactics of advance fee fraud can be traced back to the early 16th century, where face-to-face persuasion known as the 'Spanish prisoner scheme' was widely used to trick victims. Over centuries the basic scheme has adapted to new ways of communication: letters, telegraph, fax, phone or Internet. A global boost happened in the 80's with growing use of emails, enabling scammers to contact a large number of people fast and very cost efficiently. In these emails the recipient's 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"[1], 88%-90% of email traffic is considered "abusive" – unwanted or unexpected letters, or those trying to exploit the recipient. Today these schemes are also known as "419 scams", referring to the article of the Nigerian Criminal Code dealing with fraud[2]. Scammers use different story-scripts to persuade their victims to pay money upfront. An efficient script lures the victim into a fast initial payment and allows a constant flow of further payments till the victim is either broke or loses trust in the scammer. After a successful stint the scammer often re-activates a scam, usually with a follow up scheme like contacting the victim in a new role by posing as law enforcement investigating the prior scam.

Scambaiting arose as a counterattack to 419 scams. This online vigilant community of scambaiters investigates scam emails and implements several social engineering techniques to document, report or warn potential victims. Every scambaiter has his/her own personal motivation to justify their actions. As Tuovinen et. al. points out, these motives can range from community service and status elevation to revenge for being a victim of a similar scam in the past [1]. Through the documentation and sharing of these plots scambaiters waste the scammers' time, exploit their resources and raise awareness about online fraud. Yet, there are valid questions raised about ethical behavior and practices.

II. SCAMBAITING STRATEGIES

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 just by paying a little amount of money upfront. Once the receiver detects that it is a scam email, it is either deleted immediately or the email programs spam settings get adjusted. Some recipients, perhaps out of frustration or misinterpretation, take the time to reply to the scammer with messages like „please take me off your list" or „unsubscribe".

[1] http://www.maawg.org/
[2] Nigerian Criminal Code, Chapter 38: "Obtaining property by false pretenses; Cheating", http://www.nigeria-law.org/

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 the case of thescambaiter.com, which shut down in September 2011. A second reason is to emphasize that there are scambaiting methods that can be seen as anti-fraud activism rather than humiliating status elevation. The humiliating methods that do exist among scambaiters are well documented [2, 3]. Yet, by analyzing scambaiter podcast "Area 419"[3], forums like 419eater.org and thescambaiter.org, 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 realise that scambaiting is far more diverse than just humiliating the other. This list of scambaiting characteristics shows a trend of how most scammers approach potential victims and where scambaiters think action and response are needed.

A. 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; some focus on particular issues like romance scams[4], whereas others focus on scammed victims[5]. As an example it is good to take a closer look at the web forum called Scamwarners[6] (created by members of 419eater.com), where unsolicited emails and fraudulent offerings are documented. 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.

B. 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 them and lure them into incredible story-plots, constantly baiting scammers with the hope of receiving 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 a physical or virtual nature. It functions as proof of additional work or expense for the scammer. A trophy serves as evidence that the scammer believes the story-plot and had followed 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, video; a filled out form; or a check. 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 "Trophy room", "Hall of Shame"[7] or "Mugu Museum"[8]

C. The Website Reporters

Internet scammers, in order to appear professional and increase their trustworthiness, 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 by, for instance, linking DNS entries to scammer databases. They then document any illegal activities and report their findings to the hosting provider to get scammers' websites removed or banned.

The largest Internet community dedicated to stopping these activities is called "Artist against 419" (AA 419)[9], 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 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 didn't react to their requests to take down a fraudulent website. The group stopped organizing "virtual Flash mobs" and discontinued the development of those particular software programs[10] 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

[3] Area 419: Scambaiting Radio Online, blogtalkradio.com/area419
[4] Romance Scam, http://www.romancescam.com/forum/portal.php
[5] Scam Victims United, http://www.scamvictimsunited.com
[6] Scamwarners, http://www.scamwarners.com/
[7] http://forum.419eater.com/forum/album.php
[8] http://www.thescambaiter.com/photopost/
[9] http://www.aa419.org/
[10] http://wiki.aa419.org/index.php/New_Bandwidth_Policy

relationships with many hosting providers, who now use the "AA419" database to locate illegal sites and delete them from their servers[11].

D. The Bank Guards

Some scambaiters specialize in obtaining background information on all kinds of bank related issues like overpaid check validation, fake banks or closing bank accounts[12]. "Bank Guards" often target scammers who use bank accounts in their payment procedures, for e.g. charity scams. By closing bank accounts, "Bank Guards" believe that scammers lose money in a legitimate manner since bank accounts are often acquired using real names of higher ranked scammers. By documenting and reporting their criminal activities to bank officials, they monitor account transactions, freeze accounts and inform local law enforcement.

E. 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" (OD) websites to develop a personal, romantic, or sexual relationship with other people. Scammers use these sites to set up their fake profiles, often targeting single men and women who are willing to pay them money. This sort of online relationship can be a very intense experience, since the scammer will either try to get in touch with the victim on a daily basis by using multiple media channels (Email, Chat, VoIP, etc.) or send physical evidence to acknowledge his deepest love. Blinded by love, victims' pay upfront for translation fees, medical bills or visa receipts. "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 scammer's attentions and give the impression that they can be trusted easily. These scambaiters then document the scammer's practices and post their findings on victim warning forums[13] or compile stories for booklets like „hello sweaty" [4]. 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. In case of romance scams it is important to understand that dating cultures are diverse and each individual asking for financial help is not necessarily a scammer. As Jenna Burrell describes in her book „The invisible User" Africans in general face prejudices (because of West African scammers) when trying to get in contact with strangers online [5]. 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.

F. The Safari Agents

"Safari agents" are scambaiters who try to persuade the scammer into leaving his working space, so it becomes physically impossible to continue his illegal activity. As a 'rule of thumb' scambaiters either try to lure 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 workload. The scambaiter often asks for various "trophies", traces back IP-address of the e-mails that the scammer uses or utilizes other web services to confirm actual travel as a successful safari.

In May 2006 a well-documented safari ended with two scammers being sent from Lagos, Nigeria, to the violent and desolate Chad/Sudan border[14] Once there, they were to meet the rich "Reverend Belcher" 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 then went missing. This documentation provoked several discussions within the community about scambaiting ethics.

Another example is the website called "Safari Hotels Group"[15]. 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 victim's 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 to meet him.

G. The Inbox Divers

"Inbox Divers" are social engineers who harvest a scammer's email account password. They log into the scammer's email account and monitor his activities. Reading through the emails makes it easy to warn potential victims and report ongoing criminal activities. It 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 Sep 2009, a scambaiter has been collecting email addresses and passwords of scammers and providing them to his fellow scambaiters. These scambaiters then break into scammers' inboxes to monitor their practices.

III. CONCLUSIONS AND OUTLOOK

In this paper we 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

[11] http://news.cnet.com/Police-maintain-uneasy-relations-with-cybervigilantes/2100-7348_3-6150817.html

[12] http://fraudavengers.org/category/check-fraud/

[13] http://scamdigger.com/

[14] http://www.419eater.com/html/RoadToChadDarfur/

[15] http://www.safarihotelsgroup.com/

share the methods of scammers to warn other Internet users. “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 scammer’s bank accounts to officials or take fake cheques out of circulation. “Inbox Divers” infiltrate scammers’ email accounts to warn victims and document organized scamming activities.

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. The scambaiter community questions these methods and extreme cases prompt discussions about scammer ethics.

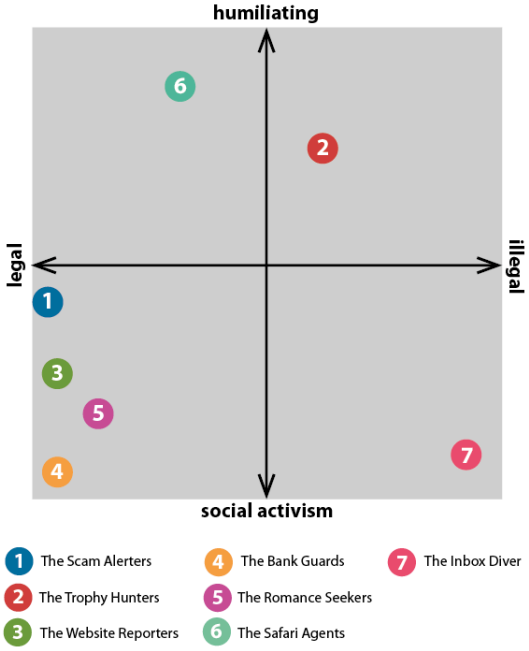

Figure 1. Diagram of scambaiting strategies

In future research, we 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 are developing a workshop and a booklet called „419 fiction - anti-fraud activism“ – a basic toolkit to get started. The aim is to present various online scams, how to identify them, introduce security strategies on how to safely navigate the Internet and to question the trustworthiness of unknown online contacts. 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

[1] Tuovinen, L. et al. 2007. Baits and beatings: vigilante justice in virtual communities. Proceedings of CEPE 2007. The 7th International Conference of Computer Ethics: Philosophical Enquiry (2007), 397–405.

[2] Krings, Matthias, 2013: Scambaiting. Ein Erzählgenre zwischen interaktiver Fiktion und Hetzjagd im Internet, in: Karl N. Renner, Dagmar v. Hoff & Matthias Krings (Hg.): *Medien - Erzählen - Gesellschaft. Transmediales Erzählen im Zeitalter der Medienkonvergenz*. Berlin: DeGruyter

[3] Cambaiter, Wayne S. Hello Sweaty. CreateSpace, 2012.

[4] Burrell, Jenna. Invisible Users: Youth in the Internet Cafés of Urban Ghana. The MIT Press, 2012