Chapter 13
Internet Crime and Anti-Fraud Activism:
A Hands-On Approach

Andreas Zingerle
Woosong University, South Korea

Linda Kronman
Woosong University, South Korea

ABSTRACT

Scambaiting is a form of vigilantism that targets internet scammers who try to trick people into advance fee payments. In the past, victims were mainly contacted by bulk emails; now the widespread use of social networking services 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, or seeking for jobs. Scambaiters are online information communities specializing in identifying, documenting, and reporting activities of scammers. By following scambaiting forums, it was possible to categorize different scambaiting subgroups with various strategies and tools. These were tested in hands-on sessions during creative workshops in order to gain a wider understanding of the scope of existing internet scams as well as exploring counter strategies to prevent internet crime. The aim of the workshops was to recognize and develop diverse forms of anti-scam activism.

INTRODUCTION

Cybercrime and online fraud are a growing phenomenon in computer-mediated communications. In 2015 the Internet Complaint Center (IC3) registered over 288,000 complaints; 127,145 reporting a loss on an average of $3,718 (FBI, 2015). In the past, victims were mainly contacted by ‘unsolicited bulk emails’: now, the widespread use of social networking services, messenger apps and heavy increase of ransomware malware has increased the possibilities for scammers to contact potential victims and infect multiple devices at once. (Bregant, and Bregant, 2014) (Edwards et al., 2017) Scambaiting arose as a counterattack to scams carried out by vigilante online communities who investigate scam emails and

DOI: 10.4018/978-1-5225-5583-4.ch013

implement several social engineering techniques to document, report or warn potential victims. (Atkins, 2013) Scambaiters are persons who reply to scam emails, being fully aware that emails are written by scammers, tricking them into believing that you are a potential victim. This means that scambaiters turn tables and lure the scammers into incredible story-plots, always giving scammers the feeling that they will get a lot of money. (Smallridge et al., 2016) Every scambaiter has their own personal motivation to justify their actions. Tuovinen et al. (2007) illustrate three possible motives: community service (social activism), status elevation and revenge. In workshops the authors emphasized the role of community service by documenting and sharing scambaiter plots, wasting time of scammers and exploiting their resources as well as raising awareness about online fraud. Scambaiting is often portrayed as a practice of humiliating the other. Lisa Nakamura (2014) argues that some of the scammers' photos resemble a 'parody of Christian baptism', whereas others remind her of 'something you have seen from Abu Ghraib', but she also points out that 'images are put out of context' and that they 'rely on users who understand the conditions under which they were created'. Still her conclusion is that the 'main purpose of scambaiting is to humiliate the other'. Often, correspondences are also hard to grasp or make no sense when put out of context since it is never clear what was communicated beforehand over email in order to receive for example a requested photo or a specific document. Dara Byrne (2013) oversimplifies that 'scambaiters are racists' and 'scambaiting tactics have never proved to be useful in crime prevention'. The author's intention is not to deny that there are subcultures within the scambaiting culture that are humiliating and show racist tendencies. Whereas prior research heavily emphasizes scambaiters motivated by status elevation and revenge, the author's interest is in understanding other sub-groups that see themselves as netizens who have a duty to provide a service to the internet community.

Over the recent years, the authors formed the 'KairUs Art+Research' (n.d.) collective and followed different vigilante communities who fight against online fraud and implemented their strategies in artistic case studies and workshops. The authors created two different workshop formats:

1. A general workshop called 'Revisiting the spam folder', where participants received an introduction into spam, scam and online vigilantism with hands-on exercises for beginning a dialog with scammers and developing story worlds using easy access online anonymization tools.
2. The 'Credible fiction – deceptive realities' workshop that builds upon artistic research conducted for the 'Megacorp.[1]'(n.d.) artwork and provided participants with a hands-on approach to collect open source intelligence about fraudulent online businesses.

The following paragraphs will take a closer look on two workshop models, different anti-fraud activist groups, and presents hands-on examples that participants were conducting during workshops.

The Workshop Models

The 'Revisiting the spam folder' workshop offered participants both a theoretical and practical introduction to narratives in fraud attempts and fictional story worlds created by scammers and scambaiters. The group sought to understand different sides of online fraud and through creative storytelling reflected on issues like online privacy, virtual representation and trust within networks. Through a 'Scam-the-Scammer Kit' (Figure 1) participants learned to create fictional online characters and infiltrated a scammers story world to observe and interrupt their workflow. Each group explored how persuasive narratives are set-up, how characters are designed and how dialog is exchanged to build trust between the acting parties. By using social media, various content generators and other tools to orchestrate internet fiction, workshop participants created entrance points to a story world and started spreading traces of information in different channels, to raise awareness about online scams and to raise issues of trust betwixt and between real and virtual. The workshop provided a base to discuss if components of scambaiting culture can be used in terms of community service in form of creative activism. Participants learned how story worlds are build, how characters are designed and dialog exchanged to build trust between actors.

Workshops were planned in two modules: a 'theoretical introduction' and 'hands-on' exercises. By introducing several scambaiting subgroups participants got to know different scam formats and strategies to unveil, disrupt and document the criminal attempts. In hands-on excercises participants had a chance to try out the introduced tactics.

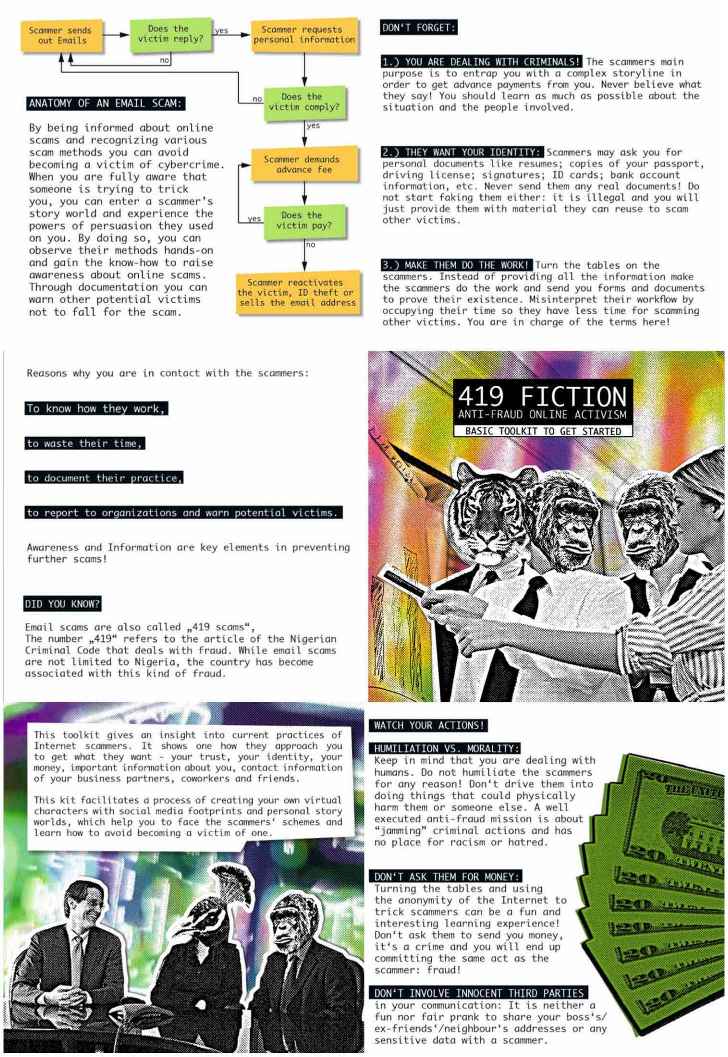
THE THEORETICAL MODULE

This part introduced participants to the history of real life scamming, starting off from early 16th century where face-to-face persuasion known as 'Spanish prisoner scheme' or 'Pig in a poke' were widely used to trick victims. Over centuries basic schemes have been 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. Participants discussed their encounters with online scams and shared strategies they knew to report or adjust spam filters. For describing different scam types the authors designed quartet cards (Figure 2) that were created as part of the artistic installation 'Re: Dakar Arts Festival' (KairUs, 2011). The cards follow the design of classic quartet cards that were originally developed for educational purposes. In a playful way, the cards raised awareness about various scam types, provided background information and offered further links to communities who fight against and report criminals. Scambait forums, investigative researchers or law enforcement all have their own methods for categorizing scams. Therefore, a challenge was to design eight categories, with four cards in every category and each card revealing a scam type, while still keeping it short and fun. Some of the cards are linked to online sources, giving yet another layer to dig deeper into the world of scamming.

After establishing a collective understanding of what scams were investigated how the world of fraud has been reflected on in different genres – ranging from pop culture to contemporary art. The authors introduced latest artistic projects and research including related artistic works such as 'Spamming back' by Christoph Schwarz, 'spam-scamscam' by Dean Cameron and Victor Isaac and 'The Scammer and scambaiter issue' by Mishka Henner. Looking at related artistic reflections on spam and scams, the authors presented artistic performances and visualizations of the phenomena.

In his work 'Spamming back' Christoph Schwarz (n.d.) plays the role of a young gallery owner, who discovers internet scammers as a new avant-garde art movement. He interprets received scam mails as part of artists' portfolios and starts selling them in his gallery. After each purchase, a polaroid photo of Schwartz and the collector is taken and immediately sent to the con-artist via email. Using the same types of promises as spammers do, he offers his services as a leading gallery in Austria, while trying to trick scammers into a contract of advanced payment at the same time. Confronting the spammers with their own strategy is the eponymous principle behind the artwork.

Figure 1. ‘Scam-the-scammer kit‘


Scammer sends out Emails
Does the victim reply?
yes
no
Scammer requests personal information
Does the victim comply?
no
yes
Scammer demands advance fee
Does the victim pay?
yes
no
Scammer reactivates the victim, ID theft or sells the email address
419 FICTION
ANTI-FRAUD ONLINE ACTIVISM
BASIC TOOLKIT TO GET STARTED

ANATOMY OF AN EMAIL SCAM:

By being informed about online scams and recognizing various scam methods you can avoid becoming a victim of cybercrime. When you are fully aware that someone is trying to trick you, you can enter a scammer’s story world and experience the powers of persuasion they used on you. By doing so, you can observe their methods hands-on and gain the know-how to raise awareness about online scams. Through documentation you can warn other potential victims not to fall for the scam.

DON‘T FORGET:

1.) YOU ARE DEALING WITH CRIMINALS! The scammers main purpose is to entrap you with a complex storyline in order to get advance payments from you. Never believe what they say! You should learn as much as possible about the situation and the people involved.

2.) THEY WANT YOUR IDENTITY: Scammers may ask you for personal documents like resumes; copies of your passport, driving license; signatures; ID cards; bank account information, etc. Never send them any real documents! Do not start faking them either: it is illegal and you will just provide them with material they can reuse to scam other victims.

3.) MAKE THEM DO THE WORK! Turn the tables on the scammers. Instead of providing all the information make the scammers do the work and send you forms and documents to prove their existence. Misinterpret their workflow by occupying their time so they have less time for scamming other victims. You are in charge of the terms here!

Reasons why you are in contact with the scammers:

To know how they work,

to waste their time,

to document their practice,

to report to organizations and warn potential victims.

Awareness and Information are key elements in preventing further scams!

DID YOU KNOW?

Email scams are also called „419 scams“,
The number „419“ refers to the article of the Nigerian Criminal Code that deals with fraud. While email scams are not limited to Nigeria, the country has become associated with this kind of fraud.

This toolkit gives an insight into current practices of Internet scammers. It shows one how they approach you to get what they want - your trust, your identity, your money, important information about you, contact information of your business partners, coworkers and friends.

This kit facilitates a process of creating your own virtual characters with social media footprints and personal story worlds, which help you to face the scammers‘ schemes and learn how to avoid becoming a victim of one.

WATCH YOUR ACTIONS!

HUMILIATION VS. MORALITY:
Keep in mind that you are dealing with humans. Do not humiliate the scammers for any reason! Don‘t drive them into doing things that could physically harm them or someone else. A well executed anti-fraud mission is about “jamming” criminal actions and has no place for racism or hatred.

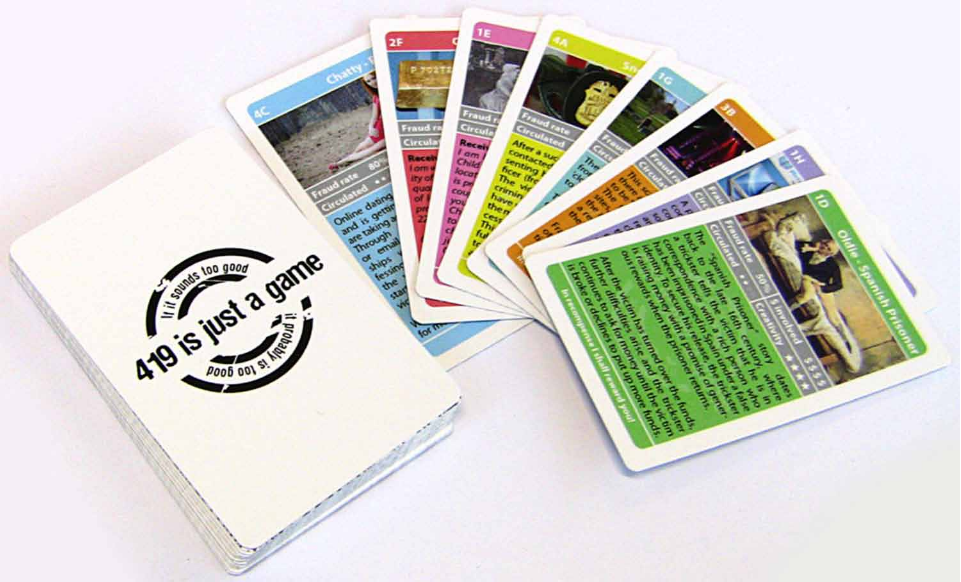
DON‘T ASK THEM FOR MONEY:
Turning the tables and using the anonymity of the Internet to trick scammers can be a fun and interesting learning experience! Don‘t ask them to send you money, it‘s a crime and you will end up committing the same act as the scammer: fraud!

DON‘T INVOLVE INNOCENT THIRD PARTIES
in your communication: It is neither a fun nor fair prank to share your boss‘s/ex-friends‘/neighbour‘s addresses or any sensitive data with a scammer.

Dean Cameron and Victor Isaac are performance artists, who perform a duologue on stage in their theatre performance ‘Spam- scamscam’ (n.d.), which is taken from the actual email correspondence with a scammer, documenting a hilarious relationship as it descends into a ‘miasma of misunderstanding, desperation, and deception’. This example illustrates well how complex storyworlds emerge from dialogs between a scammer and a scambaiter.

Mishka Henner picks up issues of the scambaiting topic in his artworks: For the photograph ‘The Skammerz Ishu’ he corresponded for a month with a scammer and directed him to pose with a Barack Obama mask (Vice, 2013). The photo and the background story were featured in the VICE magazine UK. In a second work, ‘Scambaiters’ (2014), he exhibited hand-drawn sign boards and trophy images of posing scammers taken from the 419Eater forum. Both works emphasize the humiliating side of some scambaiters and do not represent the tedious work that a lot of anti-scam activists perform against online criminals.

Figure 2. Scam quartet cards



The three works introduce the main characters; the scammer, the victim and the scambaiter, and provide a base to further discuss questions such as:

- How do scammers justify their actions?
- What makes victims reply on the most ridiculous spams?
- What motivates scambaiters?
- What tools do scambaiters use to gain the trust of scammers?
- What different strategies do scambaiters use?

The discussions were initiated through various exercises depending on the length of the workshops.

Several videos portray the scammers, victims and the scambaiting culture and its terminology and draw parallels to role playing and computer gaming culture. The authors bring up for discussion themes of trust: face-to-face vs. online, physical being vs. self-representation or real vs. the virtual. With this introduction to the world of scams, the organizers wanted the participants to try out strategies used by different scambaiting groups. In the following paragraphs the authors present scambaiting and anti-fraud activist groups, outline their main strategies and give examples how their methods were explored in the workshops.

THE PRACTICAL MODULE

The practical part of the 'Revisiting the spam folder' workshop started out by introducing the participants to a specially designed 'Scam-the-Scammer Kit' (Figure 1), a collection of tips for secure and ethical scambaiting, instructions how to start a non-traceable design of a new online identity, tools to quickly design a credible character and a story world around the bait by using transmedia storytelling methods, social media and various content generators. The participants were guided to perform a scambait either through a pre-established online narrative or through several tasks and 'missions' that allow one to design an own character within a virtual story world. The participants crafted first reply-mails to scammers and depending of the time-frame of the workshop it was also possible to receive answers from criminals. By replying to a scammers email participants started to collect background information in order to report and alert others about the scam on different web-forums. To support their warning reports, they collected evidence in form of background information or documents that were provided by the scammer.

The following paragraphs introduce different subgroups of scambaiters and their creative methods and easy to use tools that were tested out during the workshops. These subgroups include:

1. 'Scam Alerters', a group who report scam emails to warning platforms.
2. 'Trophy Hunters', a group who contact scammers in order to collect evidence that the scammer believes the scambaiters stories.
3. 'Website reporters', who host the world's largest database of fraudulent websites.
4. 'Romance scam seekers' who report fraudulent profiles on SNS and online dating platforms.
5. 'Inbox Divers', who gain access to scammers email inbox to monitor and report criminal activities.

Scam Alerters

'Alerters' identify and report online scams to increase general awareness of internet scams. They warn individuals and groups who are vulnerable to scams, providing detailed and reliable information. Furthermore, they supervise victims to protect them against follow-up scam attacks. Several websites and forums 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, ones can see that members of 419eater.com initiated it 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 already fallen for a scam, this platform provides a section with FAQs and further advice.

Workshop Exercises: Identity Creator Tools and Online Searches

Each scam narrative needs actors who engage in wild stories about stereotypical corrupt politicians and large sums of money, funds that you can claim as a next-of-kin. To show the workshop participants how scam identities are created, they were introduced to different online name generators. An 'Identity creator' (n.d.) lets you create a virtual persona within a couple of mouse clicks. By choosing parameters like gender, age, name set, and country, it is possible to create quite a plausible fake identity. It also provides random street addresses and background information like birthday, occupation, blood type, weight and height. These basic traits help when character's personality, physical appearance or soft skills are further defined. With the generated identity they were able to reply to certain emails and start collecting informations that can be posted on warning platforms.

In a second exercise the authors reversed the objective of the task, this time diving into participants spam-folders, identifying different characters and perform an online search to find background information of involved participants. Participants found several online warning platforms that focus on raising awareness on online scams and document fraudulent email accounts and phone numbers.

The Trophy Hunters

Trophy Hunters' are scambaiters who reply to scam emails, tricking internet scammers into believing they are a potential victim. These type of scambaiters aim for so called 'trophies'. A trophy - something that scambaiters acquired from scammers - can be of physical or virtual nature. It functions as proof of a scammer believing story-plots and serves as an evidence of additional work or expenses that were caused while following terms of the scambaiter. A trophy can vary depending on actual goals 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 a scambaiter manages to lure a scammer into fulfilling a time consuming and tedious task to interrupt the scammer's workflow. There are many different examples of trophies, ranging from humiliating photographs to documents that show scammer's wasted time, unveil their working practice or help to identify criminals who run the scam.

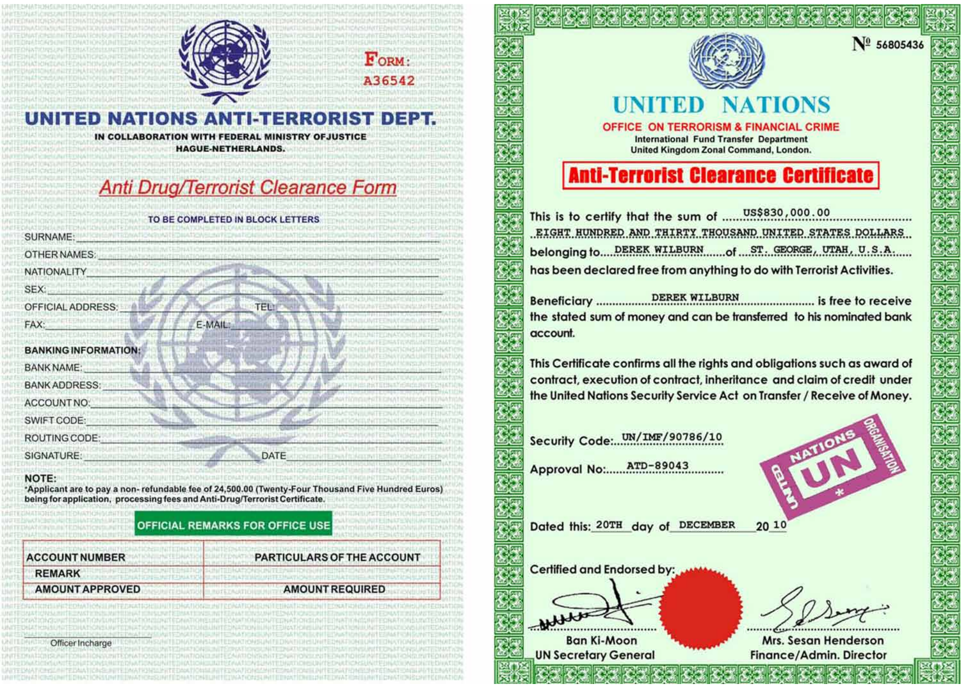
Workshop Exercise: Fake Forms

When businesses operate on an international level, administrative barriers can easily get in the way. This is a tactic often used by scammers and scambaiters for their own reasons. To appear professional and gather sensitive data, scammers use forms that victims have to fill out in order to proceed with business. Forms are taken from real companies or mimic businesses like banks, shipping traders or state institutions. Most famous bogus certificates are: 'Anti-Drug clearance form', 'Anti-Terrorist certificate' and 'Anti-Money laundering certificate'. (Figure 3) The certificates are supposedly issued by the United Nations, the International Court of Justice or by the local government in the country where business takes place. Scammers often use these certificates to request another money transfer. Scambaiters use simple forms to either waste scammers time by filling out long documents or to gain more information about scammers identities. They collect these forms as a proof that scammers believe narratives of the scambaiter. During the workshop participants were handed printouts of several forms to check which ones are real and which ones are fake. Fake forms were further discussed in which story-plots they can be used and if they would be more beneficial for scammers or scambaiters.

Workshop Exercise: Calling a Scammer

Besides filled out forms also audio recording of a more personal communication with a scammer can serve as a trophy. During an exhibition of 'Let's talk business', a scam-related artwork of the 'KairUs Art+Research' collective, several scam emails that include phone numbers were presented to the public and phone numbers that criminals used to get in direct contact were called. Once connected to a criminal, visitors were able to ask questions regarding the business proposal and discussed which further steps are necessary to continue the business. Whole conversations were recorded and considered a trophy, proofing that visitors were bold enough to talk with an online scammer. In discussions after the exercise this experience helped participants to understand that there is a real person behind the scam, something that often remains unnoticed in text based correspondence.

Figure 3. Fake 'Anti-Drug clearance form' and 'Anti-Terrorist certificate'



FORM:
A36542

UNITED NATIONS ANTI-TERRORIST DEPT.
IN COLLABORATION WITH FEDERAL MINISTRY OFJUSTICE
HAGUE-NETHERLANDS.

Anti Drug/Terrorist Clearance Form

TO BE COMPLETED IN BLOCK LETTERS

SURNAME: ____________________
OTHER NAMES: ____________________
NATIONALITY ____________________
SEX: ____________________
OFFICIAL ADDRESS: __________ TEL: __________
FAX: __________ E-MAIL: __________

BANKING INFORMATION:
BANK NAME: ____________________
BANK ADDRESS: ____________________
ACCOUNT NO: ____________________
SWIFT CODE: ____________________
ROUTING CODE: ____________________
SIGNATURE: __________ DATE __________

NOTE:
*Applicant are to pay a non- refundable fee of 24,500.00 (Twenty-Four Thousand Five Hundred Euros) being for application, processing fees and Anti-Drug/Terrorist Certificate.

OFFICIAL REMARKS FOR OFFICE USE

ACCOUNT NUMBER	PARTICULARS OF THE ACCOUNT
REMARK	
AMOUNT APPROVED	AMOUNT REQUIRED

____
Officer Incharge

Nº 56805436

UNITED NATIONS
OFFICE ON TERRORISM & FINANCIAL CRIME
International Fund Transfer Department
United Kingdom Zonal Command, London.

Anti-Terrorist Clearance Certificate

This is to certify that the sum of ......US$830,000.00...... EIGHT HUNDRED AND THIRTY THOUSAND UNITED STATES DOLLARS belonging to....DEREK WILBURN......of ....ST. GEORGE, UTAH, U.S.A....... has been declared free from anything to do with Terrorist Activities.

Beneficiary ....DEREK WILBURN.......... is free to receive the stated sum of money and can be transferred to his nominated bank account.

This Certificate confirms all the rights and obligations such as award of contract, execution of contract, inheritance and claim of credit under the United Nations Security Service Act on Transfer / Receive of Money.

Security Code:.UN/IMF/90786/10.......
Approval No:.....ATD-89043.........

UNITED NATIONS ORGANISATION
UN
*

Dated this: 20TH day of DECEMBER 20 10

Certified and Endorsed by:

Ban Ki-Moon
UN Secretary General

Mrs. Sesan Henderson
Finance/Admin. Director

Website Reporters

To appear professional and to increase their trustworthiness, 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. (Tambe Ebot, 2017) '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 hosting providers to get the websites removed or banned. The largest Internet community dedicated to stopping these activities is called 'Artist against 419' (AA419), 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 fraudulent websites 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 a whole server and not just a single website. The group provoked lots of discussions and controversy with these illegal virtual Flash Mobs, but 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)

Workshop ‘Credible Fictions: Deceptive Realities’

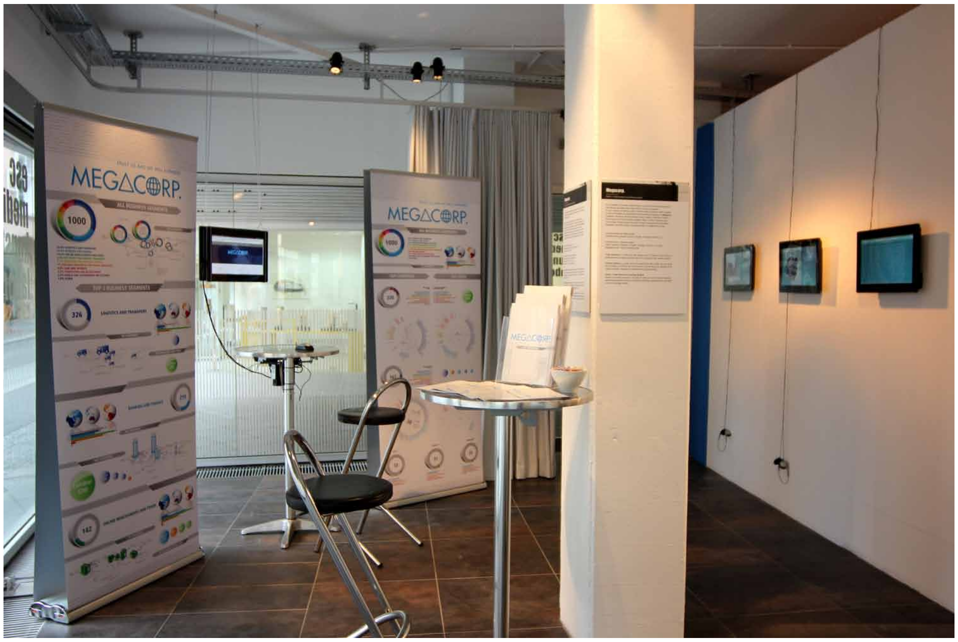
For this subcategory authors created an own workshop in which the artwork ‘Megacorp.’ by the authors served as a point of departure to further investigate Internet activism, fake websites and how ‘open source intelligence tools’ (osint) can be applied to unveil these fraudulent businesses. Companies exist only virtually and are used by cyber criminals for phishing attacks or to support scam stories. The ‘Megacorp.’ exists therefore as an umbrella company for subsidiary companies that are 100% dummy corporations. ‘Megacorp.’ operates on a global scale and is constantly growing with firms represented in almost every branch of industry. Strategic objectives according to the ‘Megacorp.’ Mission statement is to: “offer complete services from one source which can serve the entire market”. Accordingly subsidiary companies cover domestic and international export, real estate agents, insurance companies, law firms, security companies, banks, educational institutions, hospitals, online commerce, economic communities and ministries. The functions of ‘Megacorp.’ are presented in the form of an interim report and company visuals. The archived websites are locally available allowing visitors to explore the current fake website repository (Figure 4).

After the presentation of the ‘Megacorp.’ collection of fraudulent websites the authors proceeded to an exercise how to recognize fake businesses online. A checklist of osint-tools was presented to the participants, and evidence of fraud was gathered and discussed.

The checklist included:

- General look & feel of a website:
    - Are photos squeezed to fit in certain places?
    - Are logos pixelated or badly manipulated to fit into an image?

Figure 4. The ‘Megacorp.’ business conglomerate artwork



  - Are domain names spelled correctly?
  - Are contact emails same as the domain name or is it a free-to-use webmail service?
- Check freely accessible meta-data like:
  - Trade registry number,
  - VAT number or the
  - Company address and telephone number.
- A 'whois-lookup' on targeted domains can unveil when a domain was registered, most recently updated and how long this registration is valid.
- An online plagiarism checker helped to find clones of websites.
- Using a reverse 'IP-address lookup tool' it is possible to gain more insight about all different websites and domains hosted on that IP-address. Often scammers run several websites at once and it is just easier, cheaper and more convenient to host them under the same provider. This way, it is often possible to observe working methods of a group of scammers who operate several websites at once.

By applying these tools and working through a checklist, participants analyzed a website, raised the suspicion that the website is not legit and collected background information to report the suspicion to the hosting provider. Through a form the participants reported their suspicion of the fraudulent website on the AA419 forum and added it to their database. After that, it was possible to file a 'Terms of Service (TOS) and Acceptable Use Policy (AUP) Violation' report to the hosting provider, asking the abuse team to investigate the website in question with a request to take it offline as soon as possible.

Romance Scam Seekers

People use 'Social Networking Sites' (SNS) to keep in touch with family and friends or find new partners to extend their private and business networks. 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 victims on a daily basis by using multiple media channels (Email, Chat, VoIP, etc.), as well as sending physical evidence to acknowledge their deepest love. Blinded by love, victims pay upfront for translation fees, medical bills or visa fees. (Warner, 2011) '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 impressions 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' or guides like 'The Scam Survivors' Handbook' to warn potential victims (Cambaiter, 2012). They also try to track down people whose photos are used in scams and block scammers from creating more fake profiles on dating websites. In the 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 (2012) describes in her book 'The invisible Users', Africans in general face prejudices because of West African scammers when trying to contact strangers online. Several West African countries are blacklisted, and access to Online Dating, Internet Banking or Auction Sites are blocked. Denied access to information and services based on geographical location reveals unequal and undemocratic sides of the Internet.

Workshop Exercise: Exif-Data and Reverse Image Search Engines

Scammers often send images to prove their authenticity to victims. Images that come in the .jpg or .tiff format carry metadata that is stored as 'Exchangeable image file format' data (short Exif-data). When taking a photo, metadata like date, time, camera settings (e.g. camera model, aperture, shutter speed, focal length, metering mode, ISO speed), GPS location information and an image- thumbnail is saved and embedded within the image file itself. This is mostly done by default without camera owner's notice. This Exif-data is also saved in wav-audio files.

By introducing different exif-data viewers participants were able to analyze whether a photo was edited or where and when it was taken. This can often help to prove authenticity of a person or a story. Another tool to test authenticity of images is to use 'reverse image search' engines that specify finding matching images rather than finding content according to keywords, metadata or watermarks. When an image is submitted, a digital fingerprint is created that is compared to every other indexed image. Different engines and plugins vary in their accuracy, from finding similar images to exact matches including those that have been cropped, modified or resized. This way it is easily possible to analyze an image and check if the same or similar images are posted on other blogs and websites.

Inbox Divers

'Inbox Divers' are social engineers (Mann, 2010) who log into the scammers email account and warn potential victims or report ongoing criminal activities. (Krebs, 2013) Browsing through an email Inbox gives a very personal insight into 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. A scambaiter has been collecting email accounts and potential passwords of scammers and provides them to his fellow anti-scam activists. Group members then log into the scammers email account to monitor the criminals practices, warn victims and file reports.

Workshop Exercise: Analyzing a Scammers Inbox

During a workshop participants were handed out login details of a scammers email account. They were also suggested a checklist to follow while analyzing the Inbox:

1. Lookout for potential victims who are in regular contact with the scammer and believe the stories of the scammer, or even worse, are ready to pay money. These victims should be warned and are advised to stop any correspondence with the scammer.
2. Once all potential victims are warned the inbox is scanned for credit card numbers or bank account information. Account details are further reported to bank officials or credit card fraud departments

who monitor accounts. For this the scambaiter forwards a copy of scammers email including the account holder's name, bank name and address, account number, IBAN and BIC code.

3. Email accounts are often used to store email scripts, harvested email addresses, fake documents (passport templates, fake identification cards, Anti- terrorism and Drug clearance Certificates) or photos that scammers use as material to tell their stories.

These photos and documents get clearly labeled as 'FAKE' or 'used by scammers' and published on anti-fraud websites. By doing so participants were using the same forums as the 'Scam Alerters' do. In group discussions participants presented their findings and together discussed where to publish gathered information and how to proceed with infiltrated accounts.

CONCLUSION

This chapter presented individual or community-driven scambaiting and anti-fraud activists strategies that were explored in workshops for taking action against internet criminals. Lots of time and effort is invested by these groups in documenting and sharing methods of scammers to warn other internet users. 'Scam Alerters' post scam emails and give tips to victims on how to avoid further scamming schemes. Some 'Trophy Hunters' use humiliating methods like asking the scammer to send embarrassing photos, while others try to document their practice by asking for official documents, or waste the scammers time by giving them long and tedious jobs to accomplish. 'Romance scam seekers' track down scammers on online dating platforms and post findings on victim warning forums. To prove the authenticity of photographs they use reverse image search engines or analyze the images metadata. 'Website reporters' compile a register of fake web-sites and cooperate with hosting providers to get websites shut down. 'Inbox Divers' infiltrate scammers email accounts to warn victims and document organized scamming activities. Between 2013 and 2015 the authors organized more than ten workshops varying from a lecture series held at the Department of Web Sciences, University of Art and Design Linz (Austria), to full-day or half-day workshops at conferences and festivals. Shorter workshops (2-3 hours) were better suited to give an overview over different scam methods and discuss ethical issues when being in contact with Internet scammers. In longer workshops tools were presented in more detail and people had time to actively work on storytelling and corresponded with scammers. Looking at scam phenomenons from the perspectives of scammers, scambaiters, anti-fraud activists and victims enabled discussions on topics such as data security, digital divide self-representation on the web. By introducing tactics and tools that scammers and scambaiters use in their communication demystified the communities and offered a new and engaging approach to deal with them. In the workshops it was also proven that scambaiters are a far more diverse group than media as well as previous literature or artworks have been portraying them. The exercises and tools tested by the participants were found useful in recognizing fake and fraud among our daily digital stream of information. Further experimental investigations into the scambaiting subcultures are needed to determine what tools are used by groups such as 'bank guards' or 'safari agents'. (Kronman, & Zingerle, 2013) Whereas online fraud can't be totally prevented this type of workshops can be seen as an important addition to any netizens media competence skills.

REFERENCES

Atkins, B., & Huang, W. (2013). A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences*, *1*(03), 23–32. doi:10.4236/jss.2013.13004

Bregant, J., & Bregant, R. (2014). Cybercrime and Computer Crime. The Encyclopedia of Criminology and Criminal Justice.

Burrell, J. (2012). *Invisible Users: Youth in the Internet Cafes of Urban Ghana*. MIT Press. doi:10.7551/mitpress/9780262017367.001.0001

Edwards, M., Peersman, C., & Rashid, A. (2017). Scamming the scammers: towards automatic detection of persuasion in advance fee frauds. In *Proceedings of the 26th International Conference on World Wide Web Companion* (pp. 1291-1299). International World Wide Web Conferences Steering Committee.

FakeNameGenerator. (n.d.). Retrieved from: http://www.fakenamegenerator.com/

FBI. (2015). *2015 Internet crime report.* Federal Bureau of Investigation. US Department of Justice. Retrieved from: https://pdf.ic3.gov/2015_IC3Report.pdf

Henner, M. (2014). Scambaiters. *G-L.* Retrieved from: http://zkm.de/event/2015/09/globale-infosphare/g-l#mischka-henner

KairUs. (2011). RE: Dakar arts festival. *KairUs Art+Research.* Retrieved from: http://kairus.org/re-dakar-arts-festival-2011/

KairUs Art+Research. (n.d.). Retrieved from: http://kairus.org/

Krebs, B. (2013). *The Value of a Hacked Email Account*. Available: http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

Kronman, L., & Zingerle, A. (2013). Humiliating Entertainment or Social Activism? Analyzing Scambaiting Strategies against Online Advance Fee Fraud. In *Cyberworlds (CW), 2013 International Conference on*. IEEE.

Mann, I. (2010). *Hacking the human: Social engineering techniques and security countermeasures*. Gower Publishing, Ltd.

MegaCorp. (n.d.). *KairUs Art+Research.* Retrieved from: http://megacorp.kairus.org

Nakamura, L. (2014). ‘I WILL DO EVERYthing That Am Asked’: Scambaiting, Digital Show-Space, and the Racial Violence of Social Media. *Journal of Visual Culture*, 258–273.

Schwarz, C. (n.d.). *Spamming back*. Retrieved from: http://www.christophschwarz.net

Smallridge, J., Wagner, P., & Crowl, J. N. (2016). Understanding cyber-vigilantism: A conceptual framework. *Journal of Theoretical & Philosophical Criminology*, *8*(1), 57.

Spamscamscam. (n.d.). *Urgent & confidential*. Retrieved from: http://www.spamscamscam.com/

Tambe Ebot, A. C. (2017). Explaining two forms of Internet crime from two perspectives: toward stage theories for phishing and Internet scamming. *Jyväskylä Studies in Computing, 259*.

Vice. (2013). Welcome to the skammerz ishu. *Vice*. Retrieved from: https://www.vice.com/en_us/article/kwp8zz/welcome-to-the-skammerz-ishu

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *The International Journal of Cyber Criminology*, *5*, 736–749.

ADDITIONAL READING

Atta-Asamoah, A. (2009). Understanding the West African cybercrime process. *African Security Studies*, *18*(4), 105–114. doi:10.1080/10246029.2009.9627562

Blythe, M., Petrie, H., & Clark, J. A. F for fake: four studies on how we fall for phish (pp. 3469–3478). Presented at the *Proceedings of the 2011 annual conference on Human factors in computing systems*. 2011. 10.1145/1978942.1979459

Brunton, F. (2012). *Spam: a shadow history of the Internet*. MIT Press.

Rogers, M. (2003). The role of criminal profiling in the computer forensics process. *Computers & Security*, *22*(4), 292–298. doi:10.1016/S0167-4048(03)00405-X

KEY TERMS AND DEFINITIONS

Digital Storytelling: Digital storytelling describes the practice of everyday people who use digital tools such as social media, blogs, podcasts, video sharing, or email messages to tell stories. These stories can include digital narratives such as web-based stories, interactive stories, hypertexts, and narrative computer games. Many people use elaborate non-traditional story forms, such as nonlinear and interactive narratives.

Nigerian 419-Scam: 419-scam is a form of advance fee fraud that mainly uses telephone and email as a communication medium. The number 419 refers to the section of the Nigerian Criminal Code dealing with fraud, but is not limited to fraud schemes originating from Nigeria. 419-scam or "four-one-niner" became a common term for all advance fee fraud scams that are carried out over the internet, no matter whether they originate from Nigeria or from a different country.

Open Source Intelligence: Open source intelligence (osint) strategies refer to intelligence that has been derived from publicly available sources both on- and offline. It includes a wide variety of information and sources such as traditional media (radio, newspaper, tv, advertisement), web-based communities (social networking sites, wikis, blogs), publicly available government reports, company advertisement, gray and white papers, or observation and reporting. The term *open source* is not related to *open source software*.

Phishing: An attempt to get sensible information such as bank details, username and password combinations, insurance details, or credit card numbers for malicious reasons. Phishing is typically carried out in email communication by masquerading a trustworthy company and copying their corporate identity.

Scambaiting/Scambaiters/Anti-Fraud Activists: Scambaiting arose as a form of counter movement to the massive unsolicited bulk mailing of spam and scam mails. It is considered a form of online vigilantism and encompasses forms of online anti-fraud activism in order to waste the time and resources of the scammers, collectively gather information that will be of use to authorities, and publicly expose the scammer. In this thesis, the author uses both the terms *scambaiter* and *anti-fraud activist*. The term *scambaiters* refers to a very diverse group of online vigilantes, whereas *anti-fraud activist* refers to persons who take action motivated by a certain sense civic duty.

ENDNOTE

[1] "Megacorp" is a corporate conglomerate inspired by its equally powerful counterparts in science fiction. The artwork is based on a collection of fake websites scraped from internet. These companies exist only virtually and are used by cyber criminals for phishing attacks or to support scam stories.