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,