ISSN: 2451-8611
ISBN: 978-1-910172-00-1

'LET'S TALK BUSINESS' – an installation to explore scam narratives

Andreas Zingerle[1], Linda Kronman[2]

[1] University of Art and Design, Linz, Austria
andreas.zingerle@ufg.ac.at
[2] KairUs Art + Research Lab
linda@kairus.org

Abstract

16th century ‘face to face’ persuasion scams adopted to letters, telephone, fax and Internet with the development of new communication technologies. In many of today’s fraud schemes phone numbers play an important role. Various free-to-use on-line tools enable the scammers to hide their identities with fake names, bogus business websites, and VoIP services. These fake businesses or personas can appear more legitimate when connected to a phone number, enabling a faster, more personal contact to the victims. With the typology of a sample probe of 374 emails, commonly used in business proposal scams, the emails were categorized and tested to see how believable the proposals sound once the scammers were contacted by phone. The research can be explored in a 5-channel interactive audio installation called ‘Let’s talk business’ that uncovers which business proposals and scam schemes are commonly used, and how believable the proposals sound once the scammers are called.

Keywords

phone scams, audio installation, interactive storytelling, reverse engineering, artivism.

Introduction

Phone fraud can be described as a ‘fraudulent action carried out over the telephone’ and can be divided into ‘fraud against users by phone companies’ (cramming, slamming), ‘fraud against users by third parties’ (809-scams, dialer programs, telemarketing fraud, caller ID spoofing) ‘fraud against phone companies by users’ (phreaking, dial tapping, cloning) and ‘fraud against users by users’ (vishing, SMS spamming). The different fraudulent actions can also be divided into technical hacking, social hacking, and mixes of both. [4]

Curious anti-scam activists called scambaiters adapted more of the social engineering tactics to find methods to safely communicate with scammers, finding out how the scams work in order to warn potential victims. This artwork focuses on the ‘user to user fraud’ that is done by email and phone scams. Typically these scams involve storytelling and some sort of social engineering, where the fraudster creates a hyper-realistic ‘too good to be true’ situation for a mark, in order to extract sensitive data and/or money from the victim. [2] [3] These scambaiters host informative websites where scams are reported and host forums where people can discuss suspicious business proposals.

Fake businesses and personas can appear more legitimate when connected to a phone number, enabling faster and more personal contact to the victims. [1] By using services like Gmail the scammers gain access to popular VoIP services as Google talk or Skype. Additionally to this call diversion services offer scammers a way to hand out a regional phone numbers, yet answering to the calls where ever they are. These free tools enable the scammers to hide their real identities and to be in contact with the victims using fake names accompanied with diverted contact numbers. Our intention was to uncover which business proposals and scam schemes are commonly used and how believable the proposals sound once we called the scammers.

The Dataset

As a raw dataset I took a sample probe of 374 emails with phone numbers that were collected over a time period of three weeks from Nov. 11 to 30, 2014, from the ‘scammed.by’ scam email database. In 2010 this website was created under the name ‘baiter_base’, a place for scambaiting activists who document the activities of Internet scammers. The website provides a service to send in suspected scam emails, which are then automatically analyzed, categorized and published. From the emails we then extracted the phone numbers per country. The top five countries, in total 277 emails, were further categorized according to their narratives structures. Afterwards by using a VoIP service, we called scammers from some of the top five countries trying to cover a variation of the ten scam scheme types. Through this experiment we experienced that the phone conversations in comparison to the emails were very personal: some scammers were very open to explain their shady businesses, others preferred to use email and keep the phone conversation as brief as possible. Some of the scammers used voice-morphing software to anonymize their natural voices resulting in a rather creepy effect. The conversations with the scammers were recorded and some of the stories were edited and can now be listened to through the SPAM-cans in the art installation.

The Installation ‘Lets talk business’

After categorizing the scam narratives we proceeded to call the scammers. Prior to calling scammers, we wanted to know what means were necessary to stay anonymous and safe without leaving a trail that could lead to us. An interview from the ‘Area 419’ podcast series explained one method for setting up a connection to a scammer. ‘Area 419’ was a popular radio podcast that aired on a weekly basis between Feb. and Oct. 2010. (Area 419, 2010) The podcast covers background stories of the scambaiting forum 419eater.com; advice on scambaiting, including interviews with scam-activists and audio clips of phone calls with scammers. Podcast #2 includes an interview with a scambaiter called ‘SlapHappy’, who talks about his experiences with calling scammers. He uses a VoIP service and has a worldwide plan to call any landline for free. When a scammer doesn’t fully trust him in an email conversation, he calls them to build up his trustworthiness. For him it is hard to realize that there is a criminal talking on the phone, trying to persuade him to pay money. Often, the poor connection quality and the scammers’ thick accent make a conversation hard to understand. He uses the ‘cold-calling’ method to call the scammer and improvises during the conversation.

Next a VoIP account was setup under this pseudonym including a worldwide landline-calling package. The Quick Time Player software was used for recording the voices of the scammers. Before calling the scammers we created a fictional persona with name and country of origin. When a connection to a scammer was established, the scammer was informed that the email was received, but not all relevant parts fully understood, so the situation and the next steps should be explained to us once again. Then the scammers had time to explain the situation and how we should proceed further.

The installation consists of five modified SPAM-cans (see Fig.1 [C]) that are normally used to store precooked ‘SPiced hAM’ produced by the Hormel Foods Corporation. According to Merriam-Websters dictionary, the naming of unwanted mass advertisement as ‘Spam’ originates from ‘the British television series Monty Python’s Flying Circus in which chanting of the word Spam overrides the other dialogue’. The sketch premiered in 1970, but it took until the 1990s for mass emails, junk phone calls or text messages sent out by telemarketers to be called ‘spam’. [5] While most of the scam emails tend to end up in the SPAM folder, we chose to mediate these stories through physical SPAM-cans.

Contact microphones and audio players are attached to four of the cans, so that visitors can listen to the scammers’ different narratives that were recorded. The fifth device has two buttons: one button connects the visitor to a randomly chosen number from a scammers database, the other button disconnects the call. Next to the work is an information board providing instructions for talking to the scammers. With the fifth can we want to provide the visitor with an opportunity to be anonymously connected with an scammer. This is an experience of being nervous about who will answer the phone, trying to understand the narrative, and judging whether one would fall for such an offer or not. By providing instructions to the visitor, we want to pass on some guidelines and open questions that the visitor can ask the scammers. The guidelines include ‘Play along to figure out the scam’, ‘Never tell any personal information’ or ‘You are talking to criminals – still they are humans! Open questions can help the scammers to tell more about themselves or their schemes; ‘Tell me what do we do next?’, ‘How can I trust you?’ or ‘Is this operation safe?‘. On a wall next to the pedestal are two clocks indicating 'Local' and 'Nigerian' time (see Fig. 1 [A]). The best placement for the work is on a 50x50x130cm pedestal (see Fig. 1 [B]). Inside the pedestal there is a computer with an Internet connection that ables the anonymous VoIP communication between the visitor and the scammer.

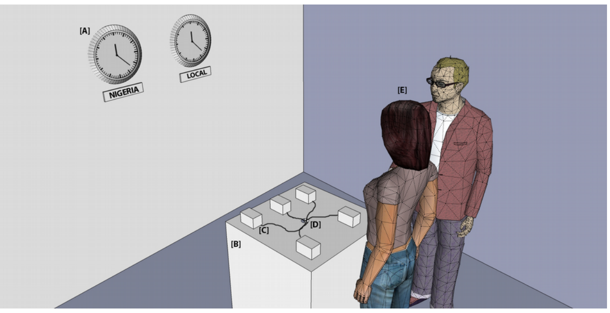

Figure 1. The installation setup

References

1. Costin, A., Isacenkova, J., Balduzzi, M., Francillon, A., & Balzarotti, D. (2013, July). *The role of phone numbers in understanding cyber-crime*. In *11th International Conference on Privacy, Security and Trust (PST 2013)*.
2. Maggi, Federico, ‘Are the con artists back? A preliminary analysis of modern phone frauds.‘ *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*. IEEE, 2010.
3. Mitnick, Kevin D, *The Art of Deception*. Wiley, 2002.
4. Rustad, M. L. (2001). *Private enforcement of cybercrime on the electronic frontier*. *S. Cal. Interdisc. LJ*, *11*, 63.
5. Templeton, B., *Origin of the term "spam" to mean net abuse*, www.templetons.com/brad/spamterm.html

Authors Biography

KairUs is a collective of two artists Linda Kronman (Finland) and Andreas Zingerle (Austria). Our work focuses on human computer and computer mediated human-human interaction with a special interest in transmedia and interactive storytelling. Since 2010 we have worked with the thematic of internet fraud and online scams. www.kairus.org