Let's talk business -
an interactive Installation to explore scam narratives

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

Linda Kronman, M.A.
Kairus Art+Research, Linz, Austria.

Abstract

16th century 'face to face' persuasion scams adapted 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. 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'.

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).

According to Rustad, these different fraudulent actions can also be divided into technical hacking, social hacking, and mixes of both.

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. (Maggi, 2010) (Mitnick, 2002) These scambaiters host informative websites where scams are reported, and 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. (Costin, 2013) By using services like Gmail the scammers gain access to popular VoIP services like Google talk or Skype. In addition to this, call diversion services offer scammers a way to hand out a regional phone numbers, yet still answer to the calls wherever they are. These free tools allow 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 we took a sample probe of 374 emails with phone numbers, which 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. Using a VoIP service, we then 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 were very personal, in comparison to the emails: 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.

	Benin	Nigeria	USA	South Africa	Burkina Faso	Total
Fund transfer	56	43	6	14	11	130
Beneficiary payment	14	13	-	1	1	29
Product selling	17	9	2	-	-	28
Follow up	9	10	5	-	-	24
Lottery Winner	8	2	4	6	1	21
Service offer	1	6	10	2	-	19
Next-of-Kin	5	3	-	-	4	12
Package found	3	3	4	-	-	10
Refugee	-	1	-	-	1	2
Orphanage	-	1	-	-	-	1
Total	113	91	31	23	18	276

Let's talk business

The installation consists of five modified SPAM-cans 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'. (Templeton) While most of the scam emails tend to end up in the SPAM folder, we chose to mediate these stories through physical SPAM-cans. Transducers 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. While most of the scam emails tend to end up in the SPAM folder we chose to mediate these stories through physical SPAM-cans.

Conclusion

The 'scammed.by' database was found to provide valuable datasets that can be further analyzed for our purposes. It offers possibilities for categorizing scam messages by scam type, country or phone carrier, which offers interesting perspectives for further investigations. When calling the phone numbers, we recognized that not all phone numbers seemed to be in use and some phone numbers appeared in several e-mails, even if the narratives or the characters' names were slightly altered. Through this experiment we experienced that the phone conversations were very personal in comparison to the emails: some scammers were very open to explaining 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 disturbing effect. The conversations with the scammers were recorded, and some of the stories were edited and can be lis- tened to through the SPAM-cans in the art installation.

Questions & Discussion

- What forms of intelligence can be gathered by being in direct contact with an Internet scammer?
- Are there moral issues that have to be considered when pretending to be a 'blue-eyed victim'?

Setup variations

- Call scammers from two or three different countries.
- Use the installation as part of a 'performance lecture'.
- Use one narrative scheme to call different scammers.

Literature cited

1. Costin, A., Isacenkova, J., Balzarsi, 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/spammeru.html