Chapter 14
Revealing Passwords:
Using Social Engineering Methods to Monitor Scammer Email Communication

Andreas Zingerle
University of Art and Design Linz, Austria

ABSTRACT

*This chapter addresses three social engineering techniques that digilante online communities of scambaiters use for 'Inbox diving': an act of gaining access to Internet scammers email accounts. The methods have been gathered by analyzing scambaiting forums and were put on the test in direct email exchange between the author and Internet scammers. By diving into the scammers' inboxes, their working methods can be observed, gang structures investigated and potential victims warned. The author discusses the moral issues an 'Inbox diver' faces and questions the ethics of scambaiting communities that prefer social engineering techniques rather than hacking email accounts. The research lead into the creation of the artistic installation 'Password: ******' and the data sculpture 'Monitoring Harry Brooks' and presents two artistic positions dealing with password security and data visualization.*

INTRODUCTION

Scammers regularly use Internet cafés as a working environment for their criminal activities (Burrell, 2012), (Warner, 2011). Besides easy access to office equipment, the scammers can also camouflage their identities and operate anonymously in the mist of other café users. Since scammers have to share the equipment with others, most of them store important documents online. The email accounts become their cloud storage where scripted messages, fake documents, harvested email addresses, login details to other accounts or gang communication with further fraudsters are saved. Law enforcement authorities find it particularly hard to catch scammers and thus gaining access to scammers' inboxes can provide valuable insights into their practices.

In April 2014 a major security bug called 'Heartbleed' was detected, allowing anyone to read the servers memory by a vulnerable version of the OpenSSL software. By doing so it was possible for at-

DOI: 10.4018/978-1-4666-8679-3.ch014

tackers to eavesdrop on various communication, read names and passwords and to impersonate services and users (Schneier, 2014). Netizens were advised to alter all their passwords after the security flaws were patched (Wood, 2014).

Recently Linkedin's and yahoo's user-login information was leaked and since people reuse passwords across multiple sites hackers could use them to access other sites (Galbraith, 2014), (Perlroth, 2012). Hacked email accounts are also used to reset passwords to other web services often resulting in identity theft (Krebs, 2014). Often, the password strength is weak and vulnerable to brute force attacks. Two-step authentication is not yet widely used and passwords are rarely changed so they can be guessed quite easily.

A subgroup of the scambaiter community enters and observes email inboxes of scammers and documents ongoing scam attempts. They use storytelling and social engineering tactics to scam the scammers consequently gaining access to their inboxes (Kronman, Zingerle, 2013). Scambaiters try to get the trust of scammers by posing as gullible victims with fake characters and compelling storytelling strategies.

Scammers and scambaiters use similar social engineering techniques and online tools to persuade the counterpart. This chapter, addresses the following issues:

- Bringing forward three case studies where scambaiters use social engineering techniques to gather sensitive data from the scammers.
- Surprisingly, so far only the methods of scammers have been discussed, yet scambaiters use similar tactics to counter fight the scammers.
- Layout moral controversies an 'Inbox diver' faces when analyzing a criminals inbox.
- Two artworks dealing with password security and inbox visualization.

SOCIAL ENGINEERING: SKILLFUL MANIPULATION OF USERS

Social engineering is defined as a 'hackers use of psychological tricks on legitimate users of a computer system, in order to obtain information he/she needs to gain access to the system' (Palumbo, 2014) rather than 'breaking into the system' (Berg, 1995). Through skillful manipulation of the human counterpart hackers avoid the security measurements that companies install to keep a system or a password secure. Similar techniques used by scammers to persuade their marks have been widely discussed (Longe, 2010), (Atkins, 2013), (Mann, 2010), (Bregant, 2014). Less attention has been given to cover social engineering techniques of scambaiters.

Method 1: Fake Form Elicitation

Scambaiters often use self-made documents to gather additional information about the scammers. During the ongoing fictional narrative baiters claim to need the forms filled out in order to continue the unfolding business preparations. These forms often resemble existing businesses e.g. local bank branches, money transfer companies or forms that follow governmental application procedures. Besides asking for personal information like full name, address or phone number they request official documents to validate the scammers identity. Figure 1 shows the fake Western Union 'Global security compliance form' and two identity cards that were submitted by a scammer. The fake forms are often used when the scammers asks the counterpart to wire money via Western Union or Moneygram: