Research on the Vital Non-Technical Factor in Telecommunications Fraud: Social Engineering

Guangxuan CHEN¹,²,a, Liping DING²,*, Guangxiao CHEN³, Guomin ZHOU¹ and Qiang LIU¹

¹Zhejiang Police College, Hangzhou, Zhejiang, China
²Institute of Software Chinese Academy of Sciences, Beijing, China
³Universidad Carlos III de Madrid, Madrid, Spain

aEmail: ericcgx@163.com
*Corresponding author

Keywords: Voice Phishing, Smishing, Social Engineering, Telecomm Fraud, Identity Theft.

Abstract. Technical factors such as pseudo base station technology, VoIP technology, Caller ID spoofing technologies are usually considered to be the key problems in telecommunications fraud. In this paper, from thousands of telecommunications fraud cases we found that social engineering attack is the vital non-technical factor behind telecommunications fraud. From appeal to authority, appeal to greed and appeal to vanity, and so on, telecommunications fraudsters (also are social engineers) usually exploit human weakness so as to influence the person to take an action that may or may not be in their best interest. And, we found the three main procedures of social engineering attacks in telecommunications fraud. Also, we provided suggestions to prevent social engineering attacks.

Introduction

Telecommunication fraud is the theft of telecommunication service (telephones, cell phones, computers etc.) or the use of telecommunication service to commit other forms of fraud [1][2][3]. In this paper, we refer telecommunications fraud to the latter, i.e., the criminal behavior that the criminals fabricate false information and set up scam to lure, cheat or threaten the victim to remit or transfer their money to the criminals through voice phishing (telephone fraud), Smishing (SMS fraud) or internet fraud. It’s a non-contact type of fraud that the victims usually don’t have the chances to face-to-face contact with the criminals who may hide in a villa in a foreign country. Even if the Chinese government has made a lot of effort to fight telecommunications fraud with the telecommunication departments and financial sectors and achieved some success, the situation is still shocking. Reports about new victims of telecommunications fraud are endless. Cunning criminals are always changing their tactics to conduct this profitable activity and evade the legal sanctions.

The data in the following pictures show the rampant and astonishing telecommunications fraud cases filed by the law enforcement departments in China in recent years. As we can see, the number of registered telecommunications fraud cases is soaring from the year 2011 to 2015, shown in Fig. 1(a). While, the money involved in the cases is increased from 4 billion to 22.2 billion, see Fig. 1(b).
The “Anti-Telecommunication Fraud Bigdata Quarterly Report” released by Tencent Guardian Program shows that the total amount of money cheated by the three types of fraud is over 3.57 billion yuan in the first quarter of 2016. Among them, voice phishing was the most serious one which involved 1.88 billion yuan, higher than the sum of money involved in smishing (720 million yuan) and internet fraud (970 million) [4], see Fig. 2.

It can be seen from the report that voice phishing is still the mainstream of fraud case, accounting for more than 50%. The proportion of smishing is increased from 10% to 26% and the money involved continues to rise in the first quarter. Smishing is actually becoming a formidable crime that no one can neglect.

What magic made the telecommunications fraud frantic and widespread as it resulted great loss to the people and the society and can evade the attack without a trace? Before, we have spent a lot of time to research the technical factors behind the telecommunications fraud, such as pseudo base station used to send spam messages, VoIP technology, Caller ID spoofing technology, and so on. However, the non-technical factors that made the victims deceived behind the telecommunications fraud are seldom concerned. In this paper, we pointed out that the social engineering attack – the way to exploit human weakness, is the vital non-technical factor behind telecommunications fraud.

**Related Work**

In the context of information security, social engineering refers to psychological manipulation of people into performing actions or divulging confidential information [5]. Social engineering is getting more and more attention among information security departments in the enterprises, organizations and governments, as it is usually adopted
by hackers in the hacking activities. Actually, the usage of social engineering has caught on among computer and information security professionals [5][6]. Kevin Mitnick, one of the most famous hackers and social engineers in the world popularized the term “social engineering” [6]. In his book “The Art of Deception: Controlling the Human Element of Security”, Kevin introduced the various social engineering attacking methods adopted by hackers and examined many example scenarios [7]. Christopher Hadnagy, American security consultant and professional social engineer, have created the world’s first framework for social engineering and introduced how malicious attackers exploit human communication and trust to obtain access to information and resources through manipulation and deceit in his book “Social Engineering: The Art of Human Hacking” [8]. Recent years, the criminals went extremes to develop the social engineering introduced by the two hacker gurus into telecommunication fraud [3]. However, the detailed discussion about social engineering behind telecommunications fraud is few. Walid Moudani and Fadi Chakik presented a fraud detection model in mobile telecommunication [9]. But most of the work is focused on technical factors.

Social Engineering in Telecommunications Fraud

What behind the countless telecommunications fraud are carefully planned conspiracies and well organized scam clans. In the early days, the fraudsters usually cast their nets around the selected area so as to cheat those who are willing to hook. Now, they have even prepared from information gathering, target selection to scams setting, so as to achieve precise attack. This is why victims are more likely to be deceived as the fraudsters know everything about them. Combined with the technical factors, the basic process of social engineering can be divided into three stages, see Fig. 3.

![Figure 3. Typical social engineering process in telecommunications fraud.](image)

Information Gathering

A successful social engineering breach begins with information gathering. Of course, this is the first rule that telecommunications fraudsters always follow. The more they know about the targets, the better they can take advantage of the targets. Aiming to the goal of “less selection and high precision”, the social engineers usually do a lot of homework before launch the attacks. That is, collect as more as possible information about the target. Table 1 lists the personal information that telecommunications fraudsters and social engineers most interest.

There are many ways for the social engineers to mine the available information. Mostly, they get the information through “passive gaining” or “active collection”. Personal information disclosure is the main way that social engineers get what they
need. Professional telecommunications fraudsters usually have “one package service” in information collection. They can buy disclosed information of a large number of people from the “upstream” or using hack technology to get the precise information of some locked people.

<table>
<thead>
<tr>
<th>Type of personal information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic information</td>
<td>Name, Sex, Age, ID, Phone number, Faith, Family information, and so on</td>
</tr>
<tr>
<td>Accounts</td>
<td>Email, Online banking accounts, Third-party payment account number, SNS account, and other online accounts for various purposes</td>
</tr>
<tr>
<td>Social relation</td>
<td>Friends, Acquaintances, Work information, and so on</td>
</tr>
<tr>
<td>Privacy</td>
<td>Address book information, Call records, SMS records, Online chats information, Personal videos, photos, Personal interests, Shopping behaviors, and so on</td>
</tr>
<tr>
<td>Online behaviors</td>
<td>Online records such as chatting, playing games, shopping and other behaviors</td>
</tr>
<tr>
<td>Other registration information</td>
<td>Real estate transactions records, Automobile trading records, Hospital records, Insurance records, and so on</td>
</tr>
</tbody>
</table>

**Information Processing**

Actually, when there is so much information available that the telecommunications fraudsters biggest task is organizing and sifting through the information acquired rather than finding extra data. The information is then classified, filtered, labelled. In order to improve the hit rate, they usually divided the potential victims into different target groups according to their information. And different attacks and tactics will imposed on them accordingly.

From now on, they begin to establish “telephone traffic group”, arrange “roles”, prepare onomastions and jargon for different scenarios. Each member in the gang will continue process the information they assigned and figure out a conversation scenario together with other members. After plenty of rehearsals, a series of vivid “life scenes” will soon display in front the innocents.

**Scams Setting**

As the information is collected and well processed, the rest is to set various scams to hook the random or carefully selected victims. It’s the process of exploiting people’s weakness according to the individual’s psychological changes that perceived by the social engineers at the moment. Victims are psychologically manipulated into performing actions (such as transfers) or divulging confidential information (such as the password of their bank accounts). The scenarios are various and techniques such as appeal to authority, appeal to greed and appeal to vanity are often adopted by the social engineer in the attacks. These scams differ from the traditional “cons” in that they are often one of many steps in a more complex fraud scheme.

When the victim is trapped in the “con games”, sometimes it is impossible for others to persuade him/her that they were conned. Tragedies are always like this that millionaire will become down-and-out in a minute. And it is too late for them to regret when they found they were deceived. Beside the technical factors such as pseudo base station technology, VoIP technology, Caller ID spoofing technology and other internet and communication technologies, the non-technical social engineering tactics such as the
exploiting of human weakness and manipulating victims into performing actions that social engineer expected are the main factors that telecommunications fraudsters always succeeds in the con games.

**Summary**
Telecommunications fraud is emerging from a variety of forms. And the scenarios are various, from appeal to authority, appeal to greed and appeal to vanity, and so on. In addition to technical factors as pseudo base station technology, VoIP technology, Caller ID spoofing technology, we point out that the social engineering is the vital non-technical factor behind the telecommunications fraud. Social engineering is a blend of science, psychology and art. It exploits human weakness. Information collection, information processing and scams setting are the main procedures of a common telecommunications fraud. Unlike overcoming the technical weakness, it’s hardly to perceive and prevent the social engineering attacks. People shouled always overcome the individual weakness and enhance security awareness, so as to better prevent social engineering attacks and telecommunications fraud.

**Acknowledgement**
In this paper, the research was sponsored by the Public Security Theory and Soft Science Research Project of Ministry of Public Security of PRC (Project No. 2015LLYJZJST035), NSFC-Zhejiang Joint Fund for the Integration of Industrialization and Informatization (Project No. U1509219) and The National High Technology Research and Development Program of China (863 Program) (Project No. 2015AA016003).

**References**