# An analysis of discourse strategies in voice phishing: government agency impersonation

Kyung Hee University
Serom Kim

**<국문 초록>**

음성을 매개로 이루어지는 보이스피싱은 일종의 언어범죄(language crime)이다(Shuy, 2005). 전화를 통한 비대면의 상황에서 사기범이 가짜 정보를 통해 범죄로 유인하고자 할 때, 피해자는 정보의 진실성을 오로지 ‘말과 대화’로 판단하게 된다. 즉, 사기범의 발화에서 나타난 특정 단어나 문장들은 범죄가 진실처럼 보이는지 아닌지를 보여주는 중요한 언어적 단서와 범죄를 성공시키기 위한 구조적 담화 전략을 지니고 있다. 그런데 보이스피싱은 피해자와 사기범이 주고 받는 대화로 이루어진다는 것에 비교해 담화분석적인 관점에서 연구가 충분히 이루어지지 않았다. 따라서 본고는 보이스피싱 대화에서 나타난 담화구조와 사기범이 이용하는 언어적 장치가 무엇인지 사회언어학적 관점에서 분석하였다. 데이터는 한국 금융감독원이 공식 홈페이지 내 ‘그놈목소리’에 기재한 보이스피싱의 실제 녹취록을 기반으로 정부기관 사칭형의 음성파일 35개를 분석하였으며 본고에서는 7가지 담화를 추려내어 기재하였다. 특히 Shuy(2005)에서 제시한 11가지 언어 범죄전략(conversational strategies in crime)의 틀에 따라 한국형 보이스피싱 범죄 담화의 특징을 비추어 본다. 분석결과 사기범은 권위적인 프레임 형성, 피해자의 관점에서 말하기, 대인관계적 입장취하기와 같은 언어전략으로 피해자에게 신뢰감을 구축한 후 협박언어를 활용하며 범죄를 단계적으로 성공시키는 담화구조를 보여주었다.

## Introduction: what is voice phishing?

Voice phishing[1] is a phone call scam to get personal information such as credit card numbers, account numbers, and pin numbers of unspecified individuals. This telecom fraud is a type of ‘language crime’ where fraudsters fabricate false discourse and set up scams via landline phone, cellphone, or other Internet communication tools to commit remote frauds, infringing on severe laypersons’ property damages (Kao et al., 2020). Since the first victim

[1] The word ‘phishing’ is a coined term of combining ‘private data’ and ‘fishing’.

case has been reported to the police in June 2006 in South Korea, the damage caused by voice phishing has been on the rise over the past years (Choung, 2008).

Also, voice phishing organizations work both domestically and overseas and they are composed of systematic structures with several departments. Research from the Korean National Police University[2] found an operational mechanism of voice phishing. According to the research, most phishing criminals belong to team-based criminal organizations, which are composed of a head office, a call center, an account opening team, a cash withdrawal team, and a currency transfer team. The general head office and call centers are mainly located in oversea countries, especially China, and the account opening team and the cash withdrawal team usually operate in South Korea. The call center members have a division of roles, such as a scenario team, a marketing team, and a computer team. In particular, the scenario team draws up false realities and conspires verbal strategies that will be used to deceive the victim. In 2015, the Seoul Provincial Police Agency arrested members of the Chinese voice phishing Call Center and confiscated more than 80 scenarios of case-by-case crime methods.[3] This proves that the members of fraudsters are using well-prepared scenarios to commit crimes. That is, a great number of voice phishing discourses are repeatedly dispersing false information targeting vulnerable groups by gender and age. The strict and systematic approaches to committing scams make potential victims harder to tell whether they are interacting with fraudsters or not. A report from the Korean Financial Supervisory Service[4] outlined voice phishing methods that have appeared so far and found they have specific method segregations tailored to gender and age groups.[5] Especially, as a basic and primary level of voice phishing, phishers impersonating companies or institutions with public trusts, such as governmental institutions, and financial companies, seek to steal personal financial information by deceiving victims who are in their 20s,30s, and the elderly with relatively little knowledge in contacting with investigative agencies.

Compared to the other types of scams, the impersonation type has several distinguishing characteristics. It can be classified as a 'protective' type of crime (Choung, 2008) where impersonating employees of the police, the prosecution, or the Financial Supervisory Service, etc., phishers stress the necessity for governmental-level protection, asserting that they can protect the victim’s personal financial information and help it not to be leaked

[2] Korean National Police University, Criminal Investigation Research, No. 2018-4, (Vol.2), p.5-6.

[3] Korean Financial Supervisory Service (FSS), Financial Supervisory Information No. 2015-30 (Vol. 843), p10.

[4] Korean Financial Supervisory Service (FSS), Financial Supervisory Information No. 2018-07 (Vol. 973), p39.

[5] Phishers target victims according to what type of frauds they are deploying. For instance fake job employment offers for men in their 20s, impersonation of government or investigative agencies for women in their 20s and 30s, mortgage fraud for people in their 40s and 50s, and virtual kidnapping for men over 50s.

anymore. Also, the research from Korean National Police University found that the criminal method has evolved into referring to names and positions of agency officials who actually work there. By referring to specific social positions and pretending as if they are investigators and prosecutors, phishers gain the upper hand at the start of a conversation. This linguistic characteristic leads them to have particular stylistic features of their crime language.

According to Lee's (2018) textlinguistic analysis of voice phishing in South Korea, unlike kidnapping or mortgage fraud types, phishers imitating investigative agents show both 'positive politeness' and 'negative politeness' (Brown and Levinson, 1987). Lee points out that their verbal tactics are characterized by the way of mixing the two politeness strategies. When phishers try not to burden the targets in carrying out actions, they show respect and courtesy by referring to the targets with the most honorific title '*kwiha'* (negative politeness) or sometimes with a pronoun of humble talk '*cehuy'* (positive politeness).

However, previous studies on voice phishing crime have mainly been concerned with legal perspectives to establish countermeasures and preventative regulations to minimize damages from voice phishing. So far, there are at least a few studies that can shed light on the linguistic features of voice phishing conversations in South Korea. Little is known of the linguistic and discoursive characteristics of voice phishing, as these have been overlooked and rarely analyzed by researchers. That is the question of how language use in voice phishing actually works still remains far from being fully answered. Also, given that no face-to-face interactions take place in the situations of voice phishing calls, victims decide the authenticity of the crime only through what phishers are talking to the victims. That is, spoken data between phishers and victims include important discoursive clues about how voice phishers delude victims and what kinds of conversational elements are deployed to serve their own ends. Thus, linguistic features of voice phishing are worth to be analyzed. Therefore, the research questions are:

(1) What are the discourse structures of voice phishing conversation?
(2) What are the conversational strategies employed by voice phishers?

## Literature review

Borrowing Shuy's (2005:6) term, voice phishing is a type of 'language crime' in which criminal activities are accomplished only through talk. Voice phishers' talk involves offering help for the benefit of targets; persuading targets to follow their commands; evidencing what they are saying; justifying what targets should do. Those are intended to achieve specific goals in the given conversational context.

Based on the observation, this study applies Shuy's (2005) 'Conversational strategies to create crime' to the context of voice phishing conversation in South Korea. Shuy (2005) examines types of conversational tactics deployed in covert investigative works by undercover police agents (U) and confidential informants (CI). He examined several cases involving spoken data elicited by U's, CI's, or information developed through police interrogations. With a qualitative approach, he closely analyzed a variety of these cases to identify strategies used by police agents to uncover underlying linguistic mechanisms of how crimes are strategically created. When CI's or U's are used to surreptitiously record potentially criminal conversations, 11 strategies of CI's or U's in creating crimes (Shuy 2005: 13-34):

(1) Being ambiguous to targets, causing them to misunderstand and therefore give the appearance of guilt
(2) Blocking targets through interrupting and overlapping their speech, as well as blocking them electronically
(3) Bringing up a topic, then changing it before the other person has a chance to respond
(4) Contaminating the tape with irrelevant things that give later listeners an impression of sleaze or illegality
(5) Camouflaging illegality with the appearance of legality
(6) Isolating targets from information that they need to know to make informed decisions
(7) Refusing to take the target's "no" for an answer
(8) Misstating something targets have said to make them appear to have said something illegal
(9) Withholding important information that the target needs to know in order to make a legitimate and legal decision
(10) Lying to targets about things that they need to know in order to decide whether to follow an illegal or a legal course of action
(11) Scripting targets to say things that would make them sound guilty

These conversational strategies to 'create' crime are relevant to analyzing the conversational context of voice phishing. For example, as in Shuy's finding, voice phishers do "speak on behalf of the target" or "camouflage illegality with the appearance of legality" in some ways to disguise criminal conduct and make targets believe them. In the view that voice phishing is a type of phone call conversation, where no physical interaction occurs, the phishers must say plausible details enough to make their crime appear to be legal acts. This indicates that there are more rooms to analyze the conversational contexts in order to determine under which circumstances victims are lured by the phishers' specific verbal strategies.

A pioneering study on voice phishing in South Korea with a linguistic perspective is Lee's (2018) textlinguistic analysis. She focuses on voice phishers' particular uses of vocabulary. According to Lee, voice phishers frequently utter specialized terms that are typically used in legal systems. As the use of specialized jargon is limited to groups in a particular field, the exclusiveness of word uses establishes an imbalance in knowledge between phishers and targets, who are laypeople in the fields. In addition, she focuses on the phishers' use of *Hanja* (漢字), Chinese characters in the voice phishing text (Lee, 2018:187). It refers to those Chinese characters borrowed from Chinese and incorporated into words with Korean pronunciation. *Hanja* is semantic-based compressed words that compress abstract or compound meanings into one *Hanja* –character. She analyzed that the phishers' choices of *Hanja*, rather than using easy Korean vernacular vocabulary, is another strategy of exposing the phishers' social status and knowledge of their impersonated identities.

## Data and methodology

This study analyzes full transcripts and actual call recordings of voice phishing conversations released by the Korea Financial Supervisory Service since 2015. The official website of the Korea Financial Supervisory Service has a 'Voice phishing protector' section where they released 488 transcripts and recordings.[6] I especially focus on an impersonation type targeting victims, who are in their 20s and 30s. The website offers 28 cases of the impersonation type of voice phishing, posted between May 2, 2018, and June 12, 2018, and this study analyzes 6 conversation extracts among them. The data are presented with Korean transcripts converted into Yale Romanization and English transcripts translated by the author.

The present study adopts discourse analysis to explain the conversational features of voice phishing and how participants are discoursively involved in criminal conversation. The discoursive approach is appropriate in analyzing the data containing turn-takings that reveal the phisher's conversational goals with strategic and conscious linguistic choices. Describing discourse strategies can help to figure out the ways how phishers deliberately plan and negotiate discourse structures (conversational agenda) over long stretches of conversation (Hansell and Ajirotutu, 1982:87).

The organization of this paper is as follows: I first show five procedures with patterned conversational trajectories of voice phishing discourses. Second, I illustrate voice phishers' conversational strategies in each of the procedures and explain linguistic features in turn exchanges between phishers and victims.

## Five procedures of voice phishing conversation

Based on Lee(2018) textlinguistic analysis, I organized five steps found in my voice phishing discourse data, especially focusing on the type of government impersonation.

[6] http://m.fss.or.kr:8000/phishingkeeper/

### Step 1: Impersonating a governmental agency

The first phisher presents specific information about his or her name, position, and affiliation as if he or she is an investigator from Korean Supreme Prosecution or police department, and then approaches victims by uttering difficult specialized terms and jargon with a coercive voice tone.

### Step 2: Threatening involvement in a crime

The phisher scares the target as if the target is involved in a serious crime, such as identity theft or personal information leaks. Then, the phisher strongly asserts that the target needs to be investigated −although the victim is in reality not involved in any crime− and tries to stand by his side when the target argues his or her innocence. Once confirming that the victims are innocent, phishers say their assets are still in danger of misappropriation. By bringing up the names of governmental agencies and their speakers' roles, the phisher persuades that he or she can take measures to protect the victim's assets. While doing so, the phisher attempts to resolve the target's suspicions under the name of protecting an innocent citizen.

### Step 3: Giving information about the crime

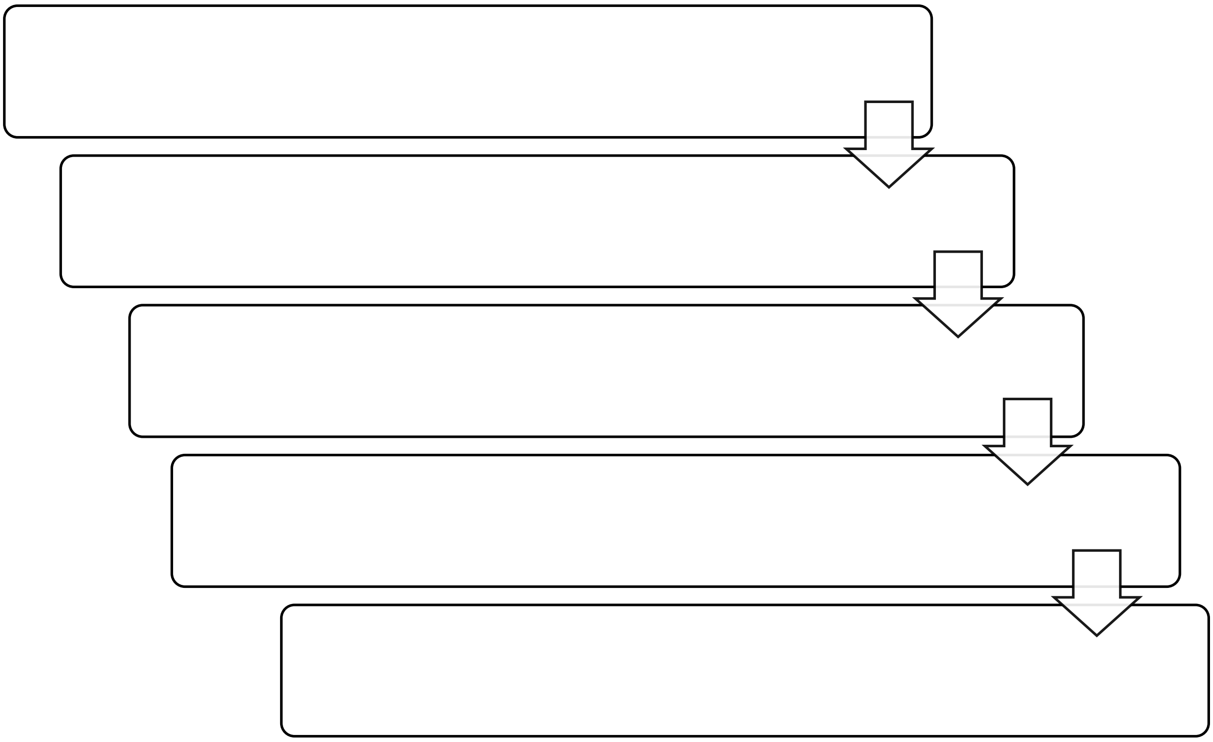
The phisher lures the target to access a fabricated website of governmental institutions, such as a prosecutors' office or a police department website. When the victim logs onto there, the phisher shows fake documents about the crimes and infects the victim's device with malware.

### Step 4: Increasing credibility

Once the first phisher performs his or her role, a second phisher impersonating another related governmental agency, such as an employee of the Financial Supervisory Service or a prosecutor, calls again and plays another role. The second phisher is the one who directs more specific procedures to the victim by commanding behaviors, such as guiding the victim into isolated spaces to block interference or assistance from third parties, directing the victim to go to the bank, to visit their office, or meet another phisher in person. By giving specific instructions and making the victim follow them, the second phisher also attempts to increase the plausibility and credibility of the crime.

### Step 5: Swindling money

The phishers guide victims by pretending to solve the problems and protect victims. The most common way of swindle is commanding the victim to transfer money to a national security account, which is in fact fabricated by the phisher's account operation team.



<Figure 1. A procedural structure of voice phishing>

## Conversational strategies

### Constructing authority frame

What’s noticeable in Lee’s analysis is that she outlines the way how phishers introduce themselves. She finds that phishers use a specifically patterned utterance composed of ' Organization + Department + (Position) + Name. This is a type of ‘informational structure’ or ‘information packaging’ (Prince, 1986), an intentional way of tailoring an utterance to meet particular assumed needs of the speaker or intended receiver. The use of a particular sequence of information is intended to catch the target’s attention and then continue their talk. The first two instances below are from Lee’s study and the last one is from my data.

(1) sewulcwungangcikem chemtanpemcoyswusa pwu ihuyna swusakwanipnita.

**Seoul Central District Prosecutors' Office, High-tech crime department, investigator Lee Hee-na.**

(2) sewulcipangkyengchalcheng kyengceypemcoyswusathim cengYY kyengsaipnita.

**Seoul Metropolitan Police Agency, Financial crime investigation team, Jeong YY.**

(3) sewulcwungangcikem kanglyekswusathim sininchel swusakwanipnita.

**Seoul Central District Prosecutors' Office, Violent crime department, I'm Detective Incheol Shin.**

By foregrounding the organization names at the very initial position of turn, the phishers take advantage of authority and reliability of the government agencies they impersonate (Lee, 2008:181). Also, the department names containing words, which sounds negative and unusual, such as ‘crime’ and ‘violence’, can arouse some possibilities of involvement in a crime directed to the target. In fact, the phishers’ actions and utterances depend on their affiliations with the governmental institutions they impersonate. Hermann(2003:190) found that a person engaging in assault, attack, and regulating the behavior of another is concerned with his or her reputation or position as the power and influence fit the profile of a threatener (Shuy, 1996). Shuy (2005:33) notes that “in the process of constructing power, the first is the basis for power negotiation. Structural power arises from the speaker’s affiliation with social institutions.” Revealing the specific profile of the phisher endows them with a related social identity that can be used as a mean for reinforcing a socially constructed identity and claiming power to control over another. This is a particular linguistic marker serving as indices of authorial positionality showing how certain a speaker or writer is perceived to be about a proposed or implicit threatening act(Gales, 2017:2). By using fake identities of governmental agencies and highlighting them at the beginning of the conversation, phishers strategically construct the asymmetric power relations in making the target comply with requests and demands. That is, this strategy is intended to establish the upper hand and superiority in the dialogue, causing obedience and fear from the target.

This conversational strategy is an initial step in constructing an authority frame. The authority frame reflects implicit expectations that participants have about behavior based on the asymmetrical relationship. Within this, the targets are subjected to a predetermined condition where their conversational roles are assumed: the phisher as an investigator versus the target as an investigation undergo-er(Lee, 2018:183). Thereby, a hierarchical relation is established between the two parties; phishers in a dominant position, whereas targets in a submissive position.

### Speaking for the target

Step 2 is important for the phishers because they have to prevent targets’ suspicions in order to proceed to their next crime steps. In case the targets show reluctance in giving additional personal information or refuse to follow the orders from phishers, they deploy more skilled strategies to evade suspicions from targets. One of the conversational strategies employed in addressing reluctance from the victims is ‘Speaking for the target’. By explicitly mentioning “voice phishing”, phishers say ‘what you might think of is voice phishing’. Data 1 and 2 below both are situations when the targets start to show doubts in terms of meeting another strange phisher in person.

**[Data 1_ 06/04/2018]**
**Victim**: animyen kuncheey kyengchalse issnuntey kase cosa patumyen antoyyo?
**Phisher**: wusenunyo, kulehkey com uykwusimi tulmyen kunyang cehuy cikemulo pangmwunul haseyyo. cikum sewulisila kulesyesscyo? sewul cikum etiey kyeyseyyo.
**Victim**: ce cikum swuwenintey.
**Phisher**: ney swuwenisilako. cehuy cikemulo pangmwunhaseyyo. kyengchal kikwanilang cehuy kemchalilang thullin kikwaninikka. saken kongmwunilatenka ta hwakinsikhye tulil kentey. yocumey mwe poisuphisingina mwe sumaysing kathun ilen kumyung pemcoy sakentul ttaymwuney kekcengul hasinun ke kathayo, kucyo? ney ponineykey mwe chwungpwunhi ku pwupwuney tayhaysenun hwakinsikhyetulillyeko hanuntey. mwe yeccweponun keey tayhayseto kiponcekin yeyuylul com kacchwusiko mwe taytapul hasyeyaci. ung? mwe com tusinun keyeyyo?
**Victim**: cikum pap mekko issessekaciko.

---

**Victim**: Or can I go to the police station nearby and have an investigation?
**Phisher**: Well, if you're that suspicious, just visit our district prosecutor’s office. You said you're in Seoul right now, right? Where are you in Seoul?
**Victim**: I'm in Suwon now.
**Phisher**: Yes, you are in Suwon. Please visit our office. We are not the same as the police agency and the prosecution. I'm gonna check all the case papers for you. **You're worried about financial crimes like voice phishing and smishing these days, right? I'd like to give you enough information about that.** You have to have some basic courtesy and answer some questions. Huh? Are you eating something?
**Victim**: I am eating right now.

Schiffrin(1993) calls the discoursive phenomena of speaking on behalf of another as “speaking for another”. One example is “making a statement about another’s internal state—something that only the other is in a position to know about” (p. 234). Her theorization is based on Goffman (1967, 1981)’s *production format*, where a speaker can be deconstructed into three roles: an *animator* who actually verbalizes or vocalizes the talk (so-called, the sounding box); an *author* who selects ideas and words to be expressed; and a *principal* who expresses his or her belief or position. He also proposes *figure* (Goffman, 1981:147), which serves as “the agent, a protagonist in a described scene, a character in an anecdote, someone, after all, who belongs to the world that is spoken about”

In terms of Goffman’s sense, interestingly, when the phisher is ‘speaking for the target’, the phisher’s language shows the use of figure in expressing ‘what he is speaking is what the target is thinking.’ The "you" is figurative, and is not synonymous with the animator, author, and principal who is speaking at present. The phisher is the animator, as he speaks the words, the phisher is also the author as his idea is expressed and the phisher is the principal in the sense that he believes the target is thinking of the call as voice phishing. However, in the phisher's turn, the target is the figure in that the phisher is positioning him in the world that is created in his talk, and in that world, the target thinks that the call is a financial scam like voice phishing. In data 2 below, the phisher utters what the target is thinking and what he is supposed to say.

**[Data 2_ 06/11/2018]**

Phisher: a hoksi mwe epmwuka manhi pappusyese mos patusin kenci animyenun ku molunun cenhwala sayngkakhasiko icey mwe poisu phisingilatunci phapilatunci ilen kumyung saki cenhwa sayngkakhasiko cikum cenhwalul an patusin kenci, hyencay cikum saken koci centali an twayssketunyo. onul nokchwi tanmal kilok hayngceng pokkwi celcha 14co 1hangey kunkehaye,

Victim: ney

---

Phisher: Oh, you didn't take the call because you were busy, or maybe you didn't answer the phone because **you thought this is a financial scam call like voice phishing**. We need to deliver the information about the case to you, but we don't record a call. Today's phone call is recorded based on Article 14 section 1 of the administrative process.

Victim: Yes.

One of the preconditions in conversation is that the one who has something to say is the one who says it. This 'speaking of yourself' rule (Schiffrin, 1993) implies conversational agreement on protecting each other's right to speak. However, by 'speaking for the target', the phishers, in fact, intercept the target's 'speaking for self' right, thereby placing the target in a powerless position whereas the phisher takes an advantageous position of staying one jump ahead of the target in the conversation. This verbal strategy is used to distance the phisher-self from "voice phishing". By doing so, the phisher seeks to not only relieve the target's doubt but also establish a foundation of offering protection for him to prevent damages from voice phishing.

## Changing topic through interpersonal stance

Shuy(2005:22) discovered a conversational strategy called 'Hit and run'. In a nutshell, it means changing a topic if the target does not say anything or react as intended. He notes, 'speakers are quite capable of changing their own topics midway through their turn of talk', meaning the occurrences of topic change contribute to eliciting the target's next moves, such as providing more information or obeying directions. The data reveals that the phishers attempt to change topics when targets show skeptical attitudes and hesitate to carry out things directed by the phishers. What is noticeable is the topics changed are mostly concerned with targets' demeanors or attitudes and the phisher aggressively blames the targets complaining his or her rudeness and impolite manner toward the phisher.

The phishers' turns initiating topic change are characterized as markers of stance as they display a variety of manifestations of interpersonal stance - a speaker's personal feelings, opinions, and attitudes about a person or proposition (Biber, 2006). Linguistic factors indicating interpersonal stance shown in phishers' turn are the degree of anger increased – high pitch sound and coercive voice tone, intensified expressions of personal emotional state – being tired and feeling offended, and modals – *will*, *have to, should*. Phishers shifts to an interpersonal stance toward targets to negotiate power, mitigate the targets' burden, and gain a foothold to step forward to the next acts. Data 5 shows the phisher complains about the target's demeanor of eating a meal while talking. Then, the phisher abruptly brings up a topic about the target's Chinese zodiac sign, the age gap between the older and the younger person.

**[Data 3_ 06/14/2018]**

Victim: cikum pap mekko issessekaciko.

Phisher: ney kiponcekin yeyuynun cikhi, cikhisyekaciko kukel hasyeyaci. OOOssi cikum wenswungitticyo?

Victim: ney

Phisher: ceyka wenswungittieyyo. phalkongnyensayng. naika manhato hancham manhun tey, kiponcekin yeyuylul kacchweya toyl ke anieyyo. kucyo? siksahasinun ken cohuntey mili com malssumul hasitenci ponin saken cinhaynghanuntey siksahasimyense ilehkey saken cinhaynghasintako, swusakwannimeykey malssum tulyesseyo?

Victim: ani kuken malssum mos tulyesseyo. coysonghapnita.

---

Victim: I am eating right now.

Phisher: Okay, **hey. Keep your basic courtesy. Mr. OOO, are you in the year of the Monkey**?

Victim: Yeah.

Phisher**: I was born in the Year of the Monkey too. I'm much older than you, so you should have some basic courtesy, right**? I don't care whether you eat or not, but did you tell the detective that you're going to eat while investigating your case?

Victim: No, I couldn't tell that. I'm sorry.

The phisher problematizes the victim's demeanor of eating while talking, saying that the phisher is older than the victim. Culturally, Korea retains its Confucianism moral norm in terms of age gap— the order in which you were born directly results in the level of respect you receive in society. By bringing up the age topic and claiming respect from the target, the phisher changes the flow of the conversation. Topic change is closely related to frame shifting. By changing the topic, the discoursive frame shifts from protection frame (protector vis-à-vis protectee) to interrelationship frame (a person vis-à-vis a person). Within this interrelationship frame, the phisher changes his footing (Goffman, 1981) from a protector to a person, who is interacting with the target as a person. Through shifting the discoursive frame, the phisher can slip through the difficulty in proceeding steps and can elicit the target’s next move. Data 6 shows that after the phisher shifts frame to the interrelationship frame, and then again returns to the protection frame where the phisher is the one investigating the target for protection.

**[Data 4_ 06/04/2018]**
Victim: ceyka mwusewese
Phisher: mweka mwusewusitanun keya. totaychey e ponini kulehkey kenpangcikey ku yaykilul haynohko e mweka kep nase kulehkey kulayyo?
Victim: ceyka honca kaya toynunkeeyyo? anim talun salamto.
Phisher: pyenhosanun kwaynchanhciman pohocanun antoypnita. pepceng nailo sengini siki ttaymwuney. kenpangcikey ilehkey thwukthwuk naypaythnun mali cikum cenun mwe salamincila mwe ung kipwun an nappacil ke kathayyo?
Victim: nappusyessulkekathayo.
Phisher: ponineykey tuk toyl key issul ke kathayyo?
Victim: kulem twusikanman kke nohumyen toyyo?
Phisher: wusen unyo. ceyka swusalul com cinhaynghakika kkelyecineyyo. ponini kyeysok mwe thwukthwuk naypaythnun maltulie solcikhi malhayse cehuy nokchwi calyoki ttaymwuney ceyka myenghwakhakey com malssum mos tulikeyssciman yeyuyka koyngcanghi epsusineyyo. chwulsekul haycwusikeysseyo? ceyka phyenuylul kulehkey pwatulinunteyto ku ponini way kulehkey malssumul hasinunci cenun ihaylul moshakeyssneyyo.

Victim: I'm afraid.
Phisher: What are you afraid of? What the hell. You've been so cocky, and, uh, you're scared of something?
Victim: Am I supposed to go alone? Or someone else.
Phisher: Your lawyer is fine, but not a guardian. because you are at the legal age of adulthood. You have spoken presumptuously. **I'm basically a human too. Don’t you think I feel unpleasant**?
Victim: You must have felt like that.
Phisher**: Do you think this will benefit you?**
Victim: So I just need to turn off my phone for two hours?
Phisher: **First of all, I feel unwilling to go ahead with this investigation. You're very rude to me. Would you visit us? I don't understand why you say like that while I am doing all the things for you.**

Within the protection frame, the phisher’s role is to persuade the target with the goal of governmental-level protection; however, within the interrelationship frame, the phisher menaces the target by saying he or she would give up the protection process. As the hierarchy in power between the two parties is established in step 1, the phisher can claim his right to be respected and to continue or give up the protection. This frame shifting is a strategic way of arousing the target in action and moving to another step in the given situation.

### Use of threatening language

FBI defines a threatening communication as a “verbalized, written, or electronically transmitted statement that states or suggests that some event will occur that will negatively affect the recipient” (Fitzgerald, 2005:2) As phishers follow the conversational trajectories, they attempt to deviate from their initial stance as a protector and frequently show stylistic features of threatening language as they are about to reach the target in person to extort cash. One of the linguistic aspects of threatening language suggested by Gales(2017) is in its use of details: the more detail or specificity used in a threat, the higher level of dangerousness(p.4). That is, high-level threats usually contain detailed descriptions of how the threat will be carried out, who is specifically targeted, and the time when the threat will occur (Napier and Mardigian, 2003).

One of the conversational strategies Shuy (2005) discovered from his study is “Camouflaging the illegality”, a form of deception where the person doing illegal actions pretends to do perfectly legal things when, in reality, they are not (p.24). He adds that since camouflaging is deliberate by its very nature, it is used by criminals to make an actual representation of illegality. It was found that the voice phishers also frequently use a similar strategy in Step 3. The phishers camouflage their illegalities by adding specific details to make their crimes sound plausible and believable. As shown in data 3, the details they use include exact time, date, names of related fraudsters, bank names, the exact amount of money, and current status of accounts, etc.

**[Data 5_ 05/02/2018]**
Phisher: cehuyka 2015nyen 7wel 5iley pwulpeptopak kunmwu sakitan iltangul ilpwu kemkehaysssupnita. kemke hyencangeyse OOOssi myenguylo toyn pwusanunhayng thongcangi palkyentoyesskwuyo, aphsen thongcangeysenun 8600manwenuy sangtanguy pwulpep topak cakumayki tuleissese tongkyelchelilul sikhyessnuntey, poninkkeysenun i kyeycwaey tayhay anun pwupwuni issusipnikka?

Phisher: On July 5, 2015, we arrested some members of the illegal gambling syndicate. An account of Busan Bank under your name of Mr.XXX was found at the scene of the arrest. The account contains 86 million-Won of illegal gambling funds. We requested freezing of the money to the bank. Do you know anything about this case?

The phisher’s description of the crime is characterized by excessive contextual details including location, time, names of doers, and related objects. That is, the phisher violates the maxim of quantity by providing too much information regarding the crime. According to Grice (1975), violation of maxims takes place “when speakers intentionally refrain to apply certain maxims in their conversation to cause misunderstanding on their participants’ part or to achieve some other purposes.” In data 4 below, the violation of quantity in the phishers turn is done mostly through listing what are impounded and who are arrested; using a chronological sequence of the current situation of the crime; exposing the specific name of the culprit.

**[Data 6_ 06/04/2018]**

Phisher: yey kulehkeyman cental patusyessko. wusenun kimca iltangul com kemkehanun kwacengeyse taylyangi poan khatu, sinyong khatu, taypho thongcangtulul com apswulul haysseyo. hyencay cwupem kimthayhwanul phohamhayse yesesmyeng kemkehan sanghwangiko acik kemketoyci anhun kumyungkwen cikwen, thongsinsa cikwen, khatusa cikwentul swusa cwungey issnun sakenipnita. acik kemketoyci anhun kongpemtuli kacang mwunceyka toynun key cekkum hayyak inchwulina yeykum inchwul kathun phihaylul iphiko hayoylo tonul seythakhanun acwu cinungcekin pemcoylul ceciluko isseyo. [...] ipen saken kimthayhwanul phohamhayse kongpemtuli kicon cenkwacaka anieyyo.

Phisher: Yes, that's what you know, we impounded some security cards, credit cards and fake bankbooks in the process of arresting the Kim-gangs. Six people have been arrested, including the main culprit, Tae-hwan Kim, and we're investigating accomplices from some financial firms, telecommunications, and credit card companies that have yet to be arrested. The accomplices committed a very intelligent crime of laundering money overseas, causing damage such as withdrawal of installment savings and deposit withdrawals. [...] The accomplices, including Kim Tae-hwan in this case, are not ex-convicts.

Vrij (2008) notes that one of the most popular verbal indicators of truthfulness is richness in detail. The richer an account is perceived to be in spatial and temporal information, names of people and places, emotions, descriptions of visions, senses, tastes, and smells, the more likely it is to be believed. That is, people perceive richness in conversational detail as an indicator of truthfulness. This, in contrast, implies a false account and the story is lack of details. Interestingly, the phishers, who are well-prepared with criminal scenario scripts in committing the crime, cover the illegality with full of details in order to make their crimes sound like true accounts. Also, an account saturated with specific details can make the victim portray specific and truthful images of the crime scene. Employing highly descriptive sentences about the crime, phishers delude the victims with false beliefs that targets are attaining shared knowledge about the crime. This, in turn, increases the targets’ involvement in the conversation, and at the same time, improves the reliability of what the phishers are doing.

# Conclusion

At the onset of this paper, I noted the current research gap in discourse analysis regarding voice phishing conversations in South Korea. As a type of ‘language crime’, where the criminal acts are committed only through verbal language in conversational interactions, the question of how voice phishers lure verbally targets and swindle money has not been answered. To fill this gap, this study identified discourive structures of voice phishing conversation and conversational strategies used by the voice phishers. It was found that impersonation types have 5 steps of procedures: impersonating a governmental agency, threatening involvement in a crime, giving information about the crime, increasing credibility, and swindling money. Unlike other types of voice phishing, impersonating investigators or prosecutors have to firm up the base of reliability on crimes so that verbal skills deployed by the criminals are developed toward the goal of plausibility and believability. I showed each of these steps contains linguistic strategies which phishers employ to complete their criminal goal. The strategies are: constructing an authority frame, speaking for the target, changing topic through interpersonal stance and use of threatening language.

Although the focus of this study is only on the impersonation type of voice phishing, it should be noted that verbal strategies of other types of phone call scams use most of the same power strategies, but not as frequently and fundamentally as they are used in the impersonation one. One reason for this may be that the identities borrowed from governmental agencies entail power asymmetries between phishers and targets. Authority coming from institutional power is the main resource for the phishers to employ in control over the target.

The conversational strategies I discovered can be used for many other types of phone call scams. I hope identifying and describing phishers' languages can not only help to clarify criminal methods of voice phishing but also help to flourish the public discussions of voice phishing conversation in South Korea and other countries.

# References

Biber, D. (2006). University language: A corpus-based study of spoken and written registers. Amsterdam: John Benjamins.

Brown, P., & Levinson, S. C. (1987). Politeness: Some universals in language usage (Vol. 4). Cambridge university press.

Choung. Wan (2008). A Legal Study of the "Voice Phishing" Fraud. Journal of Korean ciminological association, 2(2), 139-162.

Fitzgerald, J. (2005). Forensic linguistic services at the Behavioral Analysis Unit-1. Quantico, VA: FBI Academy and the National Center for the Analysis of Violent Crime.

Gales, T. (2017). Threatening Stances: a corpus analysis of realized vs. non-realized threats. Language and Law/Linguagem e Direito, 2(2).

Goffman, E. (1967). On face-work. *Interaction ritual*, 5-45.

__________ (1981). *Forms of talk*. University of Pennsylvania Press.

Grice, H. P. (1975). Logic and conversation. 1975, 41-58.

Hansell, M., & Ajirotutu, C. S. (1982). Negotiating interpretations in interethnic settings. Language and social identity, 85-94.

Hermann, M. G. (2005). Assessing leadership style: A trait analysis. The psychological assessment of political leaders, 7(2), 178-212. Ann Arbor, MI: The University of Michigan Press

Kao, Y. Y., Chen, P. H., Tzeng, C. C., Chen, Z. Y., Shmueli, B., & Ku, L. W. (2020, July). Detecting Deceptive Language in Crime Interrogation. In International Conference on Human-Computer Interaction, 80-90. Springer International Publishing

Lee, Seungah. (2018). Textlinguistic approach to the voice phishing. Textlinguistics, 45, 179-197.

Napier, M., & Mardigian, S. (2003). Threatening messages: The essence of analyzing communicated threats. Public Venue Security, 16-19.

Prince, E. F. (1986). On the syntactic marking of presupposed open propositions. In Proceedings of the 22nd Annual Meeting of the Chicago Linguistic Society

Shuy, R. W. (1996). Language crimes: The use and abuse of language evidence in the courtroom. John Wiley & Sons.

Shuy, R. W. (2005). Creating language crimes: How law enforcement uses (and misuses) language. Oxford University Press on Demand.

Vrij, A. (2008). Detecting lies and deceit: Pitfalls and opportunities. John Wiley & Sons.