Investigating (Im)politeness in Cyber Blackmail's Emails: A pragmatic Study

Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July 2021: 1354-1370

Investigating (Im)politeness in Cyber Blackmail's Emails: A pragmatic Study

Noor Saad Sabri Al Asfer

noor.s@s.uokerbala.edu.iq

Supervised By

Asst. Prof. Dr. Haider Kadhim Bairmani (Ph.D)

haider.k@uokerbala.edu.iq

University of Karbala, Department of English language, Kerbala, Iraq

ABSTRACT

There is little background available about Cyber Blackmail as a crime conducted in the space of the internet, especially for the linguistic techniques and strategies used by cyber blackmailers to convince their victims to comply with their demands. At preliminary thought, blackmailing emails might be thought of constructed out of impoliteness strategies. Yet, this is not always the case. Concerning linguistic theories, it is believed that pragmatics seems very important for revealing the way cyber blackmailers commit crimes. Hence, employing relevant pragmatic strategies might help analyze their messages and consequently the way they commit their crimes. The current study attempts to remedy the lack of attention to cyber blackmail. No study, to the researcher's best knowledge, is conducted in examining the linguistic devices of cyber blackmail, though most of the attention is placed on the legal as well as the technological methods. This study aims at investigating the types of cyber blackmail, identifying blackmailers' pragmatic strategies, and determining whether blackmailers tend to be polite or impolite in addressing their victims. It is hypothesized that most of the cases studied are of webcam (sextortion) blackmail and that cyber blackmailers employ politeness and impoliteness strategies, in which blackmailers rely on politeness strategies in addressing their victims. To achieve the study's aim and examine the hypotheses' validity, the researcher reviewed the literature of cyber blackmail, collected the study's data, i.e., emails, and developed an eclectic model to conduct the study. The study concluded that blackmailers utilize (im)politeness strategies heavily to convince and gain victims' compliance, where blackmailers employ politeness strategies more than impoliteness ones in introducing face-threatening acts.

Keywords: cyber blackmail; politeness; impoliteness; pragmatic approach; emails

1. INTRODUCTION

Language as a means of communication can be used for various purposes. One of them is to do actions; committing crimes could be one of such actions. Since the message of cyber

blackmail is transmitted via the space of the internet, the verbal method of communication is required for committing such a crime, and thus, it lies within the types of linguistic crimes. The crimes that are committed through language, as mentioned by Solan and Tiersma (2005, p.8-9) and Shuy (2005, p.6), include solicitation to murder, solicitation to sex, conspiracy, bribery, threatening, extortion (Blackmail), perjury, fraud, purchasing or selling stolen property, and presenting a false statement to government officials.

Cyber Blackmail as a cyber crime is a modern phenomenon in the research field of linguistics. Most of the research have been done to investigate the technical methodologies the criminals use in conducting their blackmail within computer science. Other studies are related to the field of law in which investigation focuses on legal issues related to the wrongful act of blackmail. To the best of the research knowledge, there is only one researcher, (Arends, 2017), who has conducted two studies on blackmail to investigate the categories of SAs under which the act of blackmail lies. Besides, there are several researches on emails conducted to investigate some other types of cyber crimes, such as fraud, in which criminals send scam emails promising for financial gain, but first, advanced payment must be submitted.

2. LITERATURE REVIEW

2.1 Cyber Blackmail

Brenner (2010, p.80) states that cyber blackmail involves the threat of publishing individuals' or companies' sensitive data obtained by the criminal unless the victim meets certain demands. A demand may include money, something of value, or extra information. Cyber blackmail, like all forms of blackmail, is a crime in all states (Content Team, 2019, para. 11). Cyber blackmail, as all cyber crimes, are dangerous and can be committed easily since cyber criminals have some advantages over ordinary ones. Juettner (2009, p.6) and Lukens (1998, p.7) have mentioned some of the privileges that cyber criminals benefit from in committing cyber crimes:

1- Cyber criminals often feel secured since they are physically distant from their victims.
2- Cyber criminals could even be respectful people who have never been convicted before.
3- Cyber crimes can attack victims located in various countries without risking being identified.
4- Cyber criminals are difficult to reach by law enforcement since they mostly leave no evidence.
5- Cyber criminals do not experience guilt in committing their crimes since they never have to meet their victims in person. They even justify their acts as something "like a business deal than like mugging someone on the street" (Juettner, 2009, p. 6).
6- No crime scene, physical evidence, or witnesses are available for conducting an investigation.
7- No means of violence is required.

The present study looks forwards to answer the following questions:

1- What types of cyber blackmail are used in emails, and which of them is the most dominant?

2- What are the politeness strategies blackmailers use, and which sub-strategies they rely on in achieving their goal?
3- What are the impoliteness strategies employed by blackmailers, and which sub-strategy is the most dominant?
4- Which method do blackmailers tend to use in conducting their blackmail, whether polite or impolite?

The following aims are sought to be achieved:

1- Identifying the types of cyber blackmail utilized by blackmailers in emails and specifying the most frequent one.
2- Investigating the politeness strategies and specifying the most frequent ones.
3- Detecting the impoliteness strategies utilized by blackmailers and finding out the most dominant sub-strategy.
4- Finding out whether blackmailers tend to be polite in their writing or impolite.

The present study hypothesizes that:

1. Webcam blackmail is the most frequently used type of cyber blackmail.
2. Blackmailers use various politeness strategies, and they rely on the off-record politeness sub-strategies in conveying their blackmail.
3. Blackmailers use various impoliteness strategies, and the most frequent one employed in constructing blackmails is the negative impoliteness sub-strategies.
4. Blackmailers tend to be polite in addressing their victims.

2.1.1 Types of Cyber Blackmail

The act of threatening an individual or a business can take various forms depending on the purpose it serves and the type of data compromised; these include emotional, webcam, or business blackmail.

2.1.1.1 Webcam Blackmail

Webcam blackmail consists of a threat for exposing any material possessed by the blackmailer, such as information, photo, or video that the victim wishes to keep private. Thus, to prevent the release of this information, he is obliged to pay the value announced by the blackmailer (Europol, 2017, p.9).

According to Mullin (2018, para. 1), Webcam Blackmail, or Sextortion, is one type of cyber blackmail in which a "fake identities" is used by the blackmailer to befriend the victims online through websites such as Skype, Facebook, or Linkedin in order to convince them to perform an act in front of the camera and then threaten to share the recording with the victim's relatives and friends unless demand for payment is met.

2.1.1.2 Business Blackmail

Sancho (2017, p.4) indicates that blackmail can be directed to individuals as well as to businesses, in which the threat is conducted to the exposure of sensitive data "unless an individual or business pays." Due to the heavy reliance on digital techniques by companies in doing their business, the cyber blackmailer has gained some advantages, i.e., being able to steal sensitive information by penetrating others' computers, hold companies at ransom beside being able to target, with a click of a mouse, a broader array of victims with impunity and without fear of being detected.

In business blackmail, blackmailers attempt to extort money from companies by threatening to share privileged information, disable critical business systems, steal intellectual property, and threaten to trade it to competitors (Ferguson & Rosencrance, 2021, para. 13-15).

2.2 Pragmatics

Pragmatics is defined by many scientists to be the focus on the meaning of an utterance outside the superficial level and its interpretation with the assistance of context. It deals with language use and the hidden meaning of an utterance in an attempt to reach the speaker's intention. It is Charles Morris who first introduced the term pragmatics as part of the theory of semiotics when he described it as the study of "the relationship of sign to interpreters" (1938, p. 6). For Leech (1983, p. 6), pragmatics is "the study of meaning in relation to speech situation," in which he asserts that the focus of pragmatics is not the language itself but the way people use language. Leech and Short (1981, p. 245) state that meaning is "derived not from the formal properties of words and constructions, but from the way in which utterances are used and how they relate to the context in which they are uttered." According to Yule (1996, p.3), pragmatics is "the study of meaning as communicated by a speaker (or writer) and interpreted by a listener (or reader)," "the study of contextual meaning," and "how more gets communicated than is said." This refers to meaning from the speaker's as well as the hearer's point of view, focusing on people's intended meaning rather than the uttered words with regard to the context as a guide to reach the unrevealed meaning. It is in this particular sense that pragmatics serves the purpose of the present study.

Additionally, Crystal (2003, p.364) states that pragmatics is about how users use language, including words and phrases' choices and the effects their language use carries to the listeners/readers during communication. The accomplishment of this process relies on the speaker, the hearer, and other elements of the context of an utterance. In the same vein, Gee (2011, p.12) focuses on the contextual elements, including participants, setting, movement, and shared knowledge in the interpretation of meaning intended by the speaker. The present study is interested mainly in two areas that serve the purposes of the current study; these include politeness and impoliteness. Politeness and Impoliteness are recent theories introduced to the field of pragmatic. They are used to assign speakers' utterances and hence intentions in addressing the hearer. The present study tries, in an attempt to find out blackmailers' tendency, to compare between blackmailers' use of these theories.

2.1.1 Politeness Theory

Politeness as a concept is intertwined with pragmatics' other theories as well as with those of persuasion. According to Lakoff (1975, p. 64), politeness is the means for reducing "friction in

personal interaction". In relation to Searle's (1975) notion of ISA, he (ibid. p.177) asserts that politeness is one of the motivations in using ISA. According to Cruse (2006, p.131), using a politeness strategy is an attempt to minimize the negative effect or the harshness of one's speech and maximize the positive effects on the receiver. It is not about information exchange; instead, it is about shaping the linguistic interaction according to social rules such as degree of friendliness (Yule, 1996, p. 59).

Brown and Levinson (1987) proposed an influential view of politeness: the Face-saving Model. The concept of Face was adopted from Goffman (1967), who states that the term Face is the "positive social value a person effectively claims for himself by the line others assume he has taken during a particular contact" (ibid. 2005, p.5). According to Brown and Levinson (1987, p.13, 61-2), face is classified into the following:

1. Positive face: the individual's "desire of being approved of".
2. Negative face: the individual's rights to be independent and non-distracted.

Certain types of SA are proved to be face-threatening; these include requests, accusations, insults, complaints, disagreements or dislikes, objections, and interruptions (Brown & Levinson, 1987, p. 65-6; Petríčková, 2012, p.12). A cyber criminal may hedge, for example, for certain reasons. He may be uncertain whether his threat would succeed in furthering his ends, i.e., making his victim comply with the demand; therefore, using hedges is one of the strategies to weaken the speaker's assertion in order to save his own face from being proved wrong later. Additionally, the blackmailer may hedge in introducing certain SAs that includes threatening the victim's face as one of the politeness strategies employed to decrease FTA. Brown and Levinson (1987, p.94-227) introduce the following politeness strategies that are used to reduce the FTAs:

2.1.1.1 Bald on-record Politeness

This strategy is used when performing FTA with maximum efficiency. When the speaker addresses the hearer directly without considering potential face damaging of the hearer, the speaker then observes the four maxims fully in which DSA is used (Brown & Levinson, 1987, p.94-5). The researcher has provided the following example:

1. Shut the door.

In this example, the speaker used an imperative sentence without any mitigation device to lessen the performance of FTA. Thus using imperative indicates going baldly on-record (Cutting, 2008, p. 46).

Bald on-record politeness strategy can be used when the speaker is superior to the hearer as in the example above, or when the performance of FTA is very slight, as in requesting, suggesting, and offering (Brown & Levinson, 1987, p.68-9).

2.1.1.2 Positive Politeness

This strategy is used for showing awareness and attention towards the hearer's want, need, etc. Brown and Levinson (1987. p.101-29) have introduced fifteen positive politeness sub-strategies as exemplified in table (1):

Table (1) *Positive Politeness sub-strategies*

No.	*Positive Politeness sub-strategies*	Example
1	Notice and attend to H (needs, wants, interests)	*"What a beautiful vase this is! Where did it come from?" (ibid. p.103)*
2	Exaggerate (Interest and sympathy with hearer)	*"What a fantastic garden you have!" (ibid. p.104)*
3	Intensify Interest to H	*"You always do the dishes! I'll do them this time." (ibid. p.107)*
4	Use in-group identity markers	*"Give us 10 rupees, sonny. I need it." (ibid. p.109)*
5	Seek agreement	*"Isn't your new car a beautiful colour!" (ibid. p.112)*
6	Avoid disagreement	*A: "Can you hear me?"* *B: "Barely." (ibid. p.114)*
7	Presuppose, assert, and raise common ground	*"I had a really hard time learning to drive, didn't I." (ibid. p.119)*
8	Joke	*"Ok if I tackle those cookies now?" (ibid. p.124)*
9	Presuppose or assert S's knowledge and concern for H's want	*"I know you can't bear parties, but this one will really be good_ do come." (ibid. p.125)*
10	Offer and promise	*"I'll drop by sometime next week." (ibid. p.125)*
11	Be optimistic	*"You'll lend me your bike, right?" (ibid. p.126)*
12	Include the S and H in an activity	*"Let's have a cookies, then." (ibid. p.127)*
13	Give (or ask for) a reason	*"Why didn't you do the dishes?!" (ibid. p.128)*
14	Assume or assert reciprocity	*"I did X for you last week, so you do Y for me this week." (ibid. p.129)*
15	Give gifts to H	*Satisfying H's want to be liked, admired, understood, cared about, listened to, and the like.) (ibid. p.129)*

2.1.1.3 Negative Politeness

It is an attempt to mitigate the FTA towards the addressee as the speaker uses politeness strategies to save the addressee's negative face. This can be done by manipulating a variety of linguistic devices, including hedges, apologies, deference, impersonalizing, etc. (Raheem, 2016, p.59). Brown and Levinson (1987, p. 129–211) have introduced ten negative politeness sub-strategies as exemplified in table (2):

Table (2) *Negative Politeness sub-strategies*

No.	*Negative Politeness sub-strategies*	Example
1	Be conventionally indirect	*"Can you please pass the salt?" (ibid. p.133)*
2	Hedge	*"You are quite right." (ibid. p.145)*
3	Be pessimistic	*"You couldn't by any chance lend me your lawnmower." (ibid. p.173)*
4	Minimize imposition	*"I just want to ask you if I can borrow a little paper." (ibid. p.177)*
5	Give deference	*"We look forward very much to dining with you." (ibid. p.181)*
6	Apologize	*"I hope you don't mind me saying this, but…" (ibid. p.188)*
7	Impersonalize S and H	*"I tell you that it is so." (ibid. p.190)*
8	State the FTA as general rules	*"The committee requests the President…" (ibid. p.207*
9	Nominalize	*"Your cooperation is urgently requested." (ibid. p.208)*
10	Go on record as a debt incurred or as a non-indebting H.	*"I could easily do it for you." (ibid. p.210)*

2.1.1.4 Off-record Politeness

This strategy is about representing acts implicitly in which the hearer's face is not threatened. Multiple interpretations are available since the speaker tends to use indirectness (Brown & Levinson, 1987, p. 211-13). They (ibid. p. 211-27) introduced fifteen off-record politeness sub-strategies as exemplified in table (3):

Table (3) *Off-record Politeness sub-strategies*

No.	*Off-record Politeness*	Example
1	Give a hint	*"It is cold in here. (c.i. Shut the window)" (ibid. p.215)*
2	Give an association clue	*"Are you going to market tomorrow?...There is a market tomorrow, I suppose. (c.i. Give me a ride there)" (ibid. p.216)*
3	Presuppose	*"I washed the car again." (ibid. p.217)*
4	Understate	*A: "What do you think of Harry?"* *B: "Nothing wrong with him. (c.i. I don't think he's very good)"(ibid. p.218)*
5	Overstate	*"There were a million people in the Co-op tonight!" (ibid. p.219)*
6	Use tautologies	*"War is war." (ibid. p.220)*
7	Use contradictions	*A: "Are you upset about that?"*

		B: "yes and no." (ibid. p.221)
8	Be ironic	*"Beautiful weather, isn't it! (to postman drenched in rainstorm)" (ibid. p.222).*
9	Use metaphors	*"Harry is a real fish. (c.i. He (drink/ swim… like a fish)" (ibid. p.222)*
10	Use rhetorical questions	*"What can I say? (c.i. Nothing, it's so bad)" (ibid. p.223)*
11	Be ambiguous	*"John's a pretty (sharp/ smooth) cookie." (ibid. p.225)*
12	Be vague	*"Looks like someone may have had too much to drink. (vague understatement)" (ibid. p.226)*
13	Over-generalize	*"Mature people sometimes help do the dishes." (ibid. p.226)*
14	Displace H	*When secretary A ask secretary B to pass the stapler where a professor is much nearer to the stapler than secretary B. Thus, the request is directed to the professor indirectly. (ibid. p.226)*
15	Be incomplete and use ellipsis	*"Well, if one leaves one's tea on the wobbly table…" (ibid. p.227)*

Thus, politeness can be defined as a language filter machine in which cruel or direct SA is being refined for the sake of maintaining good relationships and avoiding embarrassing or humiliating others.

2.1.2 Impoliteness Theory

Impoliteness is about assessing certain behavior according to negative perspectives, which are dependent on expectations, desires, and/or beliefs proposed by a social organization, such as assessing the identities of one person or group by other participants in interaction (Culpeper, 2010, p.3233). It aims at damaging the addressee's social image in which verbal aggressiveness and disharmony are caused (Culpeper et al., 2003, p.1550). In this regard, Culpeper (1996, p. 356) asserts, saying that "impoliteness super strategies are a means of attacking face."

Impoliteness is formulated from politeness as the label '(im)politeness' is proposed by Watts (2003). Culpeper (1996) derived his work of impoliteness from Brown and Levinson's theory of politeness, in which he has found out that each politeness strategy has an opposite impoliteness one with opposite orientation. He (ibid. p. 356-8) introduced these strategies as follows:

2.1.2.1 Bald on-record Impoliteness

It is a strategy in which the FTA is expressed directly, clearly, unambiguous and concise impolitely. The imperative form of the sentence is used in expressing this strategy (Culpeper, 1996, p. 356). The researcher has provided the following example:

1. Get out.

2.1.2.2 Positive Impoliteness

This strategy, with its sub-strategies, is designed to attack the positive face of the addressee. The sub-strategies, as exemplified in table (4) include the following (ibid. p. 357-8), where the researcher has provided an example for each:

Table (4) *Positive Impoliteness sub-strategies*

No.	*Positive Impoliteness*	Example
1	Ignore, snub, and fail to attend to hearer's wants, interests, needs, etc.	*I will not wait for you.*
2	Exclude the other from the activity.	*Keep away. We don't want you here.*
3	Disassociate from the other, deny common ground or association	*Do not blame me. It is your fault.*
4	Be disinterested, unconcerned, and unsympathetic	*You go and complain. I do not care.*
5	Use inappropriate identity markers	*My young fellow, did you thought that you could get away with it that easy?*
6	Use jargon and obscure or secretive language	*I do not believe that he has the magic bullet.*
7	Seek disagreement, i.e., use sensitive topics or just disagree outright (act as 'Devil's advocate')	*A: I think he may win this time.* *B: Do not count on that.*
8	Make others feel uncomfortable	*You have made my life miserable, and now it is your turn.*
9	Use taboo language, i.e., be abusive, swear, and express strong views opposed to H's	*You are so crazy.*
10	Call H names, i.e., use derogatory nominations	*Mr. James. Now everyone knows what a big loser you are.*

2.1.2.3Negative Impoliteness

These strategies are designed to damage the negative face of the addressee. They include the following sub-strategies (Culpeper,1996, p. 358), with an example for each provided by the researcher as shown in table (5):

Table (5) *Positive Impoliteness sub-strategies*

No.	*Positive Impoliteness*	Example
1	Frighten, i.e., instill the belief that action detrimental to others will occur.	*You will be sorry for this.*
2	Condescend, scorn or ridicule, i.e., emphasize own power, use diminutives to other (or other's position), be contemptuous, belittle, and do not take hearer seriously	*You are acting like a little child, you know that!*
3	Invade others' space; literally (positioning closer	*Whom have you been talking to?*

	than relationship permits) or metaphorically (ask for intimate information given the relationship.)	
4	Explicitly associate hearer with a negative aspect, i.e., personalize, use pronouns, 'I' and 'you'.	*Without me, you would not have been successful.*
5	Put H's indebtedness on record.	*You are the reason for my failure, and for your information, the failure of the son is the failure of the father.*

2.2.1.1 Sarcasm or Mock Politeness

Mock politeness is an indication of using politeness without having the intention of saving the addressee's face, in which the FTA is performed indirectly by using politeness strategies that are insincere where an implicature is constructed, as in:

2. You astonished me with your behavior.

One of the realizations of mock politeness is using 'irony', where the speaker's intention is to perform FTA. Thus, using irony does not refer to being polite since politeness flouts only on the surface of an utterance (Culpeper, 1996, p. 356; Culpeper, 2005, p. 42).

2.3 Email

Email, as the short for electronic mail, is defined by Staff (2004, p. 405) as "a means or system for transmitting messages electronically". It is mentioned in Phrasee (2016) that mailing was used in Massachusetts Institute of Technology as a program named Mailbox in 1965, in which communicators leave their messages for the next user of the same computer as the internet's service has not been invented yet. The idea has advanced on the 29th of Oct. 1969, in which an ARPANET [Advanced Research Projects Agency Network] has been executed as a network for connecting various computers across the US Department of Defense to ease communication within this organization. However, the concept of email has emerged in which the first use of email in relation to the internet dates back to 1971 thanks to the work of Ray Tomlinson, who developed his invention to include a destination for sending the email represented by the symbol @. (para. 4-15)

The frequency of emails threatening to reveal the victims' secrets to all of their contacts list for viewing adult online material unless a fee is charged has risen dramatically. The email asserts that the source has populated the computer of the recipient with spyware that has detected the contents being viewed as well as the recipient's engagement in intimate acts via webcam (Get Safe Online, n.d.,para.1). Cyber blackmailers enrich their emails by using effective strategies to make profits. For instance, the claim that the cyber criminal is hosting compromising photos or videos of sexual nature is enough to set fear within the victim resulting in forcing him to comply (Gendre, 2020, para.2,3).

Committing crimes by emails is easier than doing so by other conventional means, for it has some advantages of being easier, faster, less expensive, with the ability to attach files and the advantage

of spatial freedom and temporal versatility of emails (Palme, 1995, p.26-32, as cited in Chiad, 2010, p.13-4).

2.6.1 Using Text-based Images

The first blackmail emails were text only, but cyber criminals have modified their methods to avoid cyber security's detection mechanism using filters in identifying keywords common in blackmail. Text-based image has been used recently as an anti-detecting method where passing filters is not attainable since email filters cannot see images when scanning for signatures like malware code and URLs. (Gendre, 2020, para. 5,7)

3. FRAMEWORK

The present study is based on investigating the pragmatic strategies used by cyber blackmailers in formulating the language of their emails. It is limited to Brown and Levinson's (1987) **Politeness** theory and Culpeper's (1996) **Impoliteness** theory. The data of the study is limited to twenty-five emails collected from 2014 to 2020 from some authentic websites, where it is to be slotted into two types following Sancho's definition (2017), i.e., **Webcam Blackmail** and **Business Blackmail**. The researcher is going to adopt the following procedures in conducting the study:

1. Gathering data from some authentic websites.
2. Using Google Docs to convert the data from text-based images into texts.
3. Arranging and numbering the data in chronological order.
4. Using a mixed-method of analysis. The qualitative part is for providing full description and clarification of the theoretical side, while the quantitative one includes statistical analysis using tables of percentages and frequencies in calculating the result of analyzing the strategies used in emails.
5. Applying the eclectic model and viewing some examples of data analysis.
6. Discussing the results of the analysis.
7. Drawing conclusions to examine the validity of the hypotheses.

4. DATA ANALYSIS

Email No. 4

This email is business blackmail in which the cyber criminal is addressing a company rather than an individual. This is indicated from the following utterances, ***"please forward this email to someone in your company."*** The threat involves revealing the databases gained illegally or even selling them to those who offer the highest price. It also involves sabotaging the company's business with its client and deleting the links' indexing using the "***blackhat***" technique.

Extract 1

"(1) if you decide not to pay, (2) we will start the attack at the indicated date …;(3) you will only end up wasting more money trying to find a solution. (4) We will completely destroy your reputation amongst google and your customers."

The blackmailer threatens the victim of the consequences of ignoring his demand, trying to influence him to comply. He implies his demand within a hypothesis to leave a chance for the occurrence of the alternative decision, i.e., to meet the demand. He aims at enforcing the victim to pay in exchange for keeping business safe. In (1), he uses "*if-conditional*" in making a hypothetical meaning, employing negative politeness (hedge), rather than imposing his own opinion to minimize the effects of performing FTA as he introduces his demand for payment. Utterances (2, 3, and 4) include using negative impoliteness (frightens), where the blackmailer intends to frighten the victim of the damaging consequences to push him to meet his demand.

Email No. 6

The type of this email is webcam blackmail. This is indicated in the following utterances produced by the criminal in which he explains that he obtained the data using the victim's camera: ***"First pâit shows thē video you werē viewing', '2nd part displays the recording of your càm."***

Extract 2

"(1) You could kēep on your daily life like this nevēr happenēd (2) and you are never going to hear back again from me."

The blackmailer gives his word to the victim by promising that life will go back to normal after making the payment. Thus, he combines his request for money with the promise of ending the blackmail, where he sets the victim's compliance as a condition for ceasing the threat. Thus, he promises to leave his victim to live his life normally by employing Positive politeness (promise) in the two utterances, (1), (2), where the blackmailer appears polite as he shows awareness towards the victim's positive face by promising to leave him alone.

Email No. 8

This email is webcam blackmail. The blackmailer has gathered sensitive data concerning his victim using his camera. This is indicated from the following utterance: ***"I collected all your private data and I recorded you through your webcam".***

Extract 3

"(1) The only way to stop me, (2) is to pay exactly 800$ in Bitcoin (BTC)."

The blackmailer introduces the condition for stopping the threat as the only way to get out of this situation, i.e., to accept the deal and pay the amount. He tries to drive the victim to comply where no other safe choice is available. In (1), he resorts to imply his demand in order

to minimize FTA using off-record politeness (hint), as he suggests for the victim to stop the threat. In (2), The blackmailer employs negative politeness (generalize), where he implies his request without specifying the victim as the addressee to minimize FTA towards the victim's negative face.

5. DISCUSSION

This section includes discussing the result of analyzing the twenty-five email as a whole, along with providing frequencies and percentages of occurrences within tables.

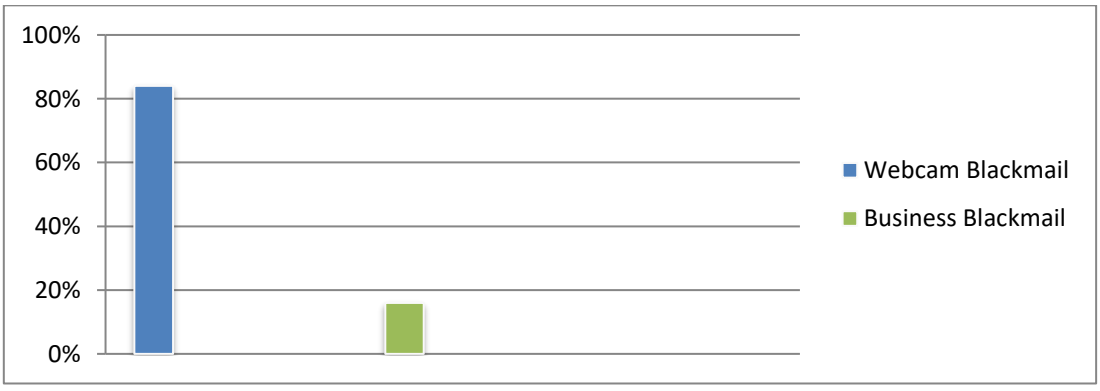
5.1 Types of Cyber Blackmail's Results Discussion

Data analysis has shown that most of the emails are of webcam type, where the blackmailers have captured victims' intimate data and use them as a hostage to obtain money for exchange. Twenty-one emails out of twenty-five are webcam blackmails, which occupies (84%), whereas only four emails are business blackmails, which occupies (16%). It is believed that webcam blackmail has higher occurrence than business blackmail due to the easiness of the method used to obtain such data, merely by spreading malware on some websites, i.e., a specific harmful electronic virus that infects computers, resulting in the victims' computers and all of the accounts controlled by the cyber criminals. Table (1) and figure (1) illustrate the occurrence of cyber blackmail's types:

Table (1) ***Types of Cyber Blackmail***

No.	Types of Cyber Blackmail	Fr.	Pr.
1	**Webcam Blackmail**	**21**	**84%**
2	**Business Blackmail**	**4**	**16%**
Total		**25**	**100%**

Figure (1) ***Types of Cyber Blackmail***



5.2 Politeness's Results Discussion

Frequencies and percentages of using politeness strategies are distributed differently among their sub-classification. Off-record politeness occupies the first place with the frequency of

(332) and the percentage of (50.2%), where hint as a sub-strategy has the highest frequency and percentage among other Off-record sub-strategies, i.e., (232), (69.9%). Thus, blackmailers appear to be polite since they go off-record while revealing their goal of the emails. Negative politeness occupies the second place with the frequency of (205) and percentage of (30.9%), where Hedge as a sub-strategy has the highest frequency and percentage among other sub-strategies, i.e., (185), (90.2%). Blackmailers again appear to be polite as they try to minimize FTA through using mitigation words, i.e., hedges. Positive politeness occupies the third place with the frequency of (116) and a percentage of (17.5%). It is detected through using promise as a sub-strategy with the frequency of (62) and the percentage of (53.45%), and (attend H's needs) with the frequency of (21) and the percentage of (18.1%) where blackmailers show awareness toward victims positive face, thus, appear polite.

Finally, Bald on-record politeness (imperative) occupies the last place with the frequency of (9) and percentage of (1.36%). Table (2) illustrates the result of detecting politeness strategies in emails:

Table (2) ***Politeness Strategies in Emails***

No.	Politeness	Sub-strategies	Fr.	Pr.
1	**Bald on-record politeness**	**Imperative**	**9**	**100%**
	Total		**9**	**1.36 %**
2	**Positive Pol.**	**Attend H's needs**	**21**	**18.1%**
		Promise and offer	**62**	**53.45%**
		Be optimistic	**10**	**8.62%**
		Seek agreement	**6**	**5.17%**
		Give reason	**18**	**15.5%**
		Intensify interest to H	**1**	**0.86%**
		Sympathizes	**4**	**3.45%**
		Include both S and H in an activity	**2**	**1.7%**
		Give gift	**2**	**1.7%**
	Total		**116**	**17.5%**
3	**Negative** politeness	**Hedge**	**185**	**90.2%**
		Apologies	**5**	**2.44%**
		Minimize imposition	**6**	**2.9%**
		State FTA as a general rule	**4**	**1.95%**
		Go on record as a debt	**2**	**0.98%**
		Be pessimistic	**3**	**1.46%**
	Total		**205**	**30.9%**
4	**Off-record** politeness	**Hint**	**232**	**69.9%**
		Give association clue	**58**	**17.47%**

		RQ	**28**	**8.4%**
		Tautology	**1**	**0.3%**
		Displace H	**3**	**0.9%**
		Use ellipsis	**5**	**1.5%**
		Presupposes	**4**	**1.2%**
		Understate	**1**	**0.3%**
	Total		**332**	**50.2%**
Total			**662**	**100%**

5.3 Impoliteness's Results

Results have shown that blackmailers use impoliteness strategies with different frequencies and percentages and these strategies are distributed differently among their sub-classification.

Negative impoliteness occupies the first place with the frequency of (337) and percentage of (76.6%), where the sub-strategies Personalize, Invade H's space, and Frighten, among other Negative Politeness's sub-strategies, have the highest frequencies and percentages as follow: (147), (43.62%), (89), (26.4%), (80) (23.74%). Here, blackmailers intend to threaten victims' negative faces by addressing them using the pronoun 'you' and speaking about victims' personal information to indicate the coming of evil consequence and to frighten them.

Bald on-record impoliteness (imperative) occupies the second place with the frequency of (78) and the percentage of (17.7%), where blackmailers direct their victims to obey their demand without any attempt to preserves victims' faces.

Mock politeness occupies the third place with the frequency of (20) and the percentage of (4.5%), where blackmailers use irony to indicate insincere politeness

The last place is occupied by Positive politeness (ignores H's need), where it has the frequency of (5) and the percentage of (1.14%). Table (3) illustrates the results of detecting impoliteness strategies in emails:

Table (3) ***Impoliteness Strategies in Emails***

No.	**Impoliteness**	Sub-strategies	Fr.	Pr.
1	**Bald on-record** impoliteness	**Imperative**	**78**	**100%**
	Total		**78**	**17.72%**
2	**Positive** impoliteness	**Ignores H's need**	**5**	**100%**
	Total		**5**	**1.14%**
3	**Negative** impoliteness	**Frighten**	**80**	**23.74%**
		Condescend and Ridicule	**21**	**6.23%**
		Invade H's space	**89**	**26.4%**
		Personalize	**147**	**43.62%**

	Total		**337**	**76.6%**
4	**Mock** politeness	**Irony**	**20**	**100%**
	Total		**20**	**4.54%**
Total			**440**	**100%**

6. Conclusion

Cyber blackmailers usually blackmail victims using their embarrassing data as a hostage that is obtained through their webcam on which they gained control using the virus that victims' computers have been infected with during visiting adult websites. Thus, most of the cases studied are of Webcam or Sextortion types.

Cyber blackmailers employ both polite and impolite strategies in their emails. However, they rely on politeness strategies in introducing their demand and in conveying the threat to reduce the impact of performing FTA. Off-record politeness serves the purpose as blackmailers use indirectness during using some SA that carries a threat to victims' faces. Negative impoliteness is used as blackmailers shift their tone to impoliteness to remind victims of the consequence of rejecting the blackmail. However, cyber blackmailers tend to use a polite method of communicating. One justification is that they have to succeed in altering the thinking of their victims and convincing them of the necessity of making the payment. Thus, they must be polite as a means of being convincing.

References

1. Arends, J. (2017a). The Felicity Conditions of Blackmail. [An Unpublished Term Paper]. Department of Linguistics, University of Amsterdam. Netherlands.
2. _____, (2017b). Blackmail: How does it Works. [M.A. Thesis]. Retrieved from https://scripties.uba.uva.nl/download?fid=650721
3. Brenner, S. W. (2010). *Cybercrime: criminal threats from cyberspace*. ABC-CLIO.
4. Brown, P. & Levinson, S. C. (1987). *Politeness*: *Some Universals in Language Usage* (2nd ed.). Cambridge: Cambridge University Press.
5. Chiad, M. O. (2010). Conventional Correspondences and E-mails: Distinguishable Text Types: A Comparative Study. [An Unpublished Ph.D. Dissertation]. University of Pune. Institute of Advanced Studies in English.
6. Cruse, A. (2006). *Glossary of semantics and pragmatics*. Edinburgh University Press.
7. Crystal, D. (2003). *A Dictionary of Linguistics and Phonetics* (5th ed.). Oxford: Blackwell.
8. Culpeper, J. (1996). Towards an anatomy of impoliteness. *Journal of Pragmatics 25*(3), 349–367. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/0378216695000143
9. ———. Bousfield, D., & Wichmann, A. (2003). Impoliteness revisited: with special reference to dynamic and prosodic aspects. *Journal of Pragmatics, 35*(10-11), 1545-1579. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0378216602001182
10. ———. (2005). Impoliteness and Entertainment in the Television Quiz Show: The Weakest Link. *Journal of Politeness Research, 1*(1), 35–72. Retrieved from https://www.researchgate.net/publication/249931038_Impoliteness_and_Entertainment_in_the_Television_Quiz_Show_The_Weakest_Link
11. ———. (2010). Conventionalised impoliteness formulae. *Journal of pragmatics*, *42*(12), 3232-3245. Retrieved from https://www.researchgate.net/publication/223412233_Conventionalized_Impoliteness_Formulae
12. Cutting, J. (2008). *Pragmatics and discourse: A resource book for students*. London: Routledge.

13. Gee, J. P. (2011). *How to do discourse analysis: A toolkit*. New York: Routledge.
14. Goffman, E. (1967). *Interaction ritual: Essays in face-to-face behavior*. Chicago, IL: Aldine Publishing Company.
15. Juettner, B. (2009). *Crime Scene Investigations: Blackmail and Bribery*. San Francisco CA: Gale Engage Learning.
16. Lakoff, R. (1975). *Language and woman's place*. New York: Harper & Row.
17. Lukens, R. J. (1998). *A critical handbook of children's literature* (2nd ed.). DIANE Publishing.
18. Leech, G. N. (1983). *Principles of pragmatics*. London: Longman.
19. _____. & Short M. H., (1981). *Style in Fiction. A linguistic Introduction to English Fictional Prose.* London: Longman.
20. Morris, C. H. (1938). Foundation of the theory of signs. In *International Encyclopedia of Unified Science*, *2*(1). Chicago: University of Chicago Press.
21. Palme, J. (1995). *Electronic Mail.* Artech House: Boston.
22. Petríčková, I. (2012). Politeness strategies in interview questions. Bachelor"s Diploma Thesis. Czech: Masarykova University. Retrieved from https://is.muni.cz/th/zqdds/Thesis.pdf
23. Raheem, K. M. (2016). A Pragmatic Analysis of Politeness Strategies in Some Selected Presidential Debates. Retrieved from https://www.researchgate.net/publication/349176741_Pragmatic_Analysis_of_Politeness_Strategies_in_Some_Selected_Presidential_Debates.
24. Sancho, D., (2017). Digital extortion: A forward-looking view. *Trend Micro Forward-Looking Threat Research (FTR) Team*. Retrieved from https://documents.trendmicro.com/assets/wp-digital-extortion-a-forward-looking-view.pdf
25. Searle, J. (1975). *Indirect Speech Acts*, in Peter Cole and Jerry L. Morgan(eds.). *Syntax and Semantics* 3: Speech Acts, Academic Press.
26. Shuy, R. W. (2005). *Creating language crimes: How law enforcement uses (and misuses) language*. Oxford University Press on Demand.
27. Solan, L. M., & Tiersma, P. M. (2005). *Speaking of crime: The language of criminal justice*. University of Chicago Press.
28. Watts, R. J., (2003). *Politeness*. Cambridge University Press.
29. Staff, M. W. (2004). *Merriam-Webster's collegiate dictionary*, 2. Merriam-Webster.
30. Yule, G. (1996). *Pragmatics*. Oxford: Oxford University Press.

Websites

1. Content Team, (2019). Blackmail. In Legal Dictionary. Retrieved from https://legaldictionary.net/blackmail/. [Accessed on 17 Jan. 2021]
2. Europol. (2017). Online sexual coercion and extortion as a form of crime affecting children: law enforcement perspective. European Cybercrime Centre. Retrieved from https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children_0.pdf. [Accessed on 16 Jan. 2021]
3. Ferguson, K. & Rosencrance, L., (2021). Cyberextortion. Retrieved from https://searchsecurity.techtarget.com/definition/cyberextortion. [Accessed on 3 Feb. 2021]
4. Gendre, A. (2020). The Evolution of Sextortion Emails. Vade Secure. Retrieved from https://www.vadesecure.com/en/blog/the-evolution-of-sextortion-emails. [Accessed on 29 Jan. 2021]
5. Get Safe Online: Free Expert Advice, (n.d.). Blackmail Emails. Retrieved from https://www.getsafeonline.org/protecting-yourself/blackmail-emails/. [Accessed on 29 Jan. 2021]
6. Mullin, G. (2018), The Sun: What is Sextortion?. Retrieved from https://www.thesun.co.uk/news/2293628/sextortion-how-common-is-webcam-blackmail-and-how-to-keep-yourself-safe-online-latest/. [Accessed on 16 Jan. 2021]
7. Phrasee. (2016). A brief history of email: dedicated to Ray Tomlinson. Retrieved from https://phrasee.co/blog/a-brief-history-of-email/. [Accessed on 30 Jan. 2021]