UNIVERSIDAD DE SALAMANCA

FACULTAD DE FILOLOGÍA

GRADO EN ESTUDIOS INGLESES

Trabajo de Fin de Grado

Unveiling Scam Messages: a Forensic Linguistic Analysis of Scam Messages

Alumno/a: Lucía Chana Fernández
Tutora: María Jesús Sánchez Manzano

Salamanca, 2024

UNIVERSIDAD DE SALAMANCA

FACULTAD DE FILOLOGÍA

GRADO EN ESTUDIOS INGLESES

Trabajo de Fin de Grado

Unveiling Scam Messages: a Forensic Linguistic Analysis of Scam Messages

This thesis is submitted for the degree of English Studies

Date: July 2024

Tutora: María Jesús Sánchez Manzano

Signature

Firmado por SANCHEZ MANZANO MARIA JESUS - 07821119S el día 02/07/2024 con un certificado emitido por AC FNMT Usuarios

Abstract

This TFG is based on the importance of using forensic linguistics to analyse scam messages. Through a forensic linguistic analysis, the main objective is to identify the specific linguistic characteristics of different scam messages, which can be considered as danger markers and can be used in the future for risk assessment so as to be able to prevent similar and potentially criminal cases. This study is limited to pointing out whether there are linguistic markers or patterns that determine fraudulent messages, and to see the importance of forensic linguistics when carrying out this particular kind of study, which is currently going to have a great impact owing to the great proliferation of this type of scams through the connectivity that new technologies provide us with.

Key words

Forensic linguistics, scam messages, linguistic characteristics, danger markers, linguistic patterns

Resumen

Este Trabajo de Fin de Grado se basa en la importancia del uso de la lingüística forense a la hora de analizar mensajes fraudulentos. A través de un análisis lingüístico forense, el objetivo principal es identificar las características lingüísticas específicas de diferentes mensajes estafa, las cuales pueden llegar a considerarse marcadores de peligro y utilizarse en un futuro para la evaluación de riesgos a la hora de prevenir casos similares y potencialmente delictivos. Este estudio se limita a señalar si existen o no marcadores o patrones lingüísticos determinativos de los mensajes fraudulentos, y ver la importancia de la lingüística forense a la hora de realizar este tipo de estudios que en la actualidad van a tener una gran repercusión debido a la gran proliferación de este tipo de estafas a través de la conectividad que las nuevas tecnologías nos proporcionan.

Palabras clave

Lingüística forense, mensajes fraudulentos, características lingüísticas, marcadores de peligro, patrones lingüísticos

Index

Introduction

Forensic linguistics is a relatively new science of applied linguistics. The term first appeared in the discourse analysis of the Evans' case in the United Kingdom in 1949. Linguistics Professor Jan Svartvik (1968) published a book entitled *The Evans Statements: A Case for Forensic Linguistics*, in which the term was used for the first time. This book analyses Evans' statements when he turns himself in for the murder of his wife and his 14-month-old daughter. At trial, Evans accused his neighbour John Christie of committing the murders, but eventually confessed to both murders, albeit with notable inconsistencies between the first declaration and the final one, radically changing the vocabulary used. The first confession was made in a more colloquial vocabulary, while the second confession denoted a formal written register, with police and institutional language, which may have hinted at the police pressure he was under to confess. Evans was sentenced to death in 1950, and three years after his execution, his neighbour Christie confessed to both murders and to the murders of several other women, including his wife. Evans was posthumously pardoned in 1966, this case helped to abolish capital punishment in the United Kingdom and the application of linguistics on the legal field.

Svartvik's work (1968) shows a new role for applied linguistics, taking a much more active role in society than the hitherto widespread one, which was only devoted to the study and teaching of languages. But, as the definition of forensic linguistics indicates, it is a discipline or branch of applied linguistics that oversees analysing the relationships that exist between language and the legal sphere. Although this relationship between language and law did not have an assigned term from the beginning, we could speak of forensic linguistics thousands of years ago with the first legal compilations created, subsequently with them we began to unite language with the legal field. This was also indicated by the author David Mellinkoff (1963) which initiated the development of this linguistic field for the first time, although it did not have a specific name until five years later with the previously mentioned work of Svartvik.

As mentioned above, forensic linguistics is a language science that has a brief history, dating back to the 1960s. But it was in the 1990s, with the creation of the International Association of Forensic Linguists (IAFL), the International Association for Forensic Phonetics and Acoustics (IAFPA), and the journal Forensic Linguistics: The International Journal of Speech, Language and the Law (IJSLL), that forensic linguistics

experienced great growth. These organisations have led to forensic linguistics gaining worldwide recognition and consolidation as a new language discipline. Thanks to this recognition, many linguists specialised in this field, and numerous related articles, and seminars began to proliferate. The extensive study carried out in these three decades has helped us to establish new patterns when analysing judicial evidence, determining the authorship of texts, verifying speakers through phonetic patterns, or analysing the authenticity of a text (a subject that we will later develop in this study), among many other functions that forensic linguistics performs today.

This paper is going to deal with the importance of forensic linguistics on scam messages that are being perpetrated over the internet; hence, the current digital era and the connectivity it provides to a global level mean that many people are trying to take advantage of it and obtain some type of benefit, giving rise to numerous ways of deceiving people through a medium that we all have at our disposal. Cybercrime is something that has been reported to the competent authorities since the beginning of the 21st century and the commence of the digital era, this concept refers to all activities of dubious legality, or illegitimate, that take place through electronic media and technologies, or, as Bossler and Berenblum (2019, 1) note "cybercrime can therefore be viewed as a large umbrella term that encompasses computer-assisted crime in which computers and technology are used in a supporting role". But the term cybercrime encompasses many forms of screen-based crime, as McGuire and Dowling (2013) enumerate, such as viruses and malwares, worms, trojans, spywares, hackings, and spams among others forms, this last one being the one in which this paper is going to be parsed. Cybercrime is complicated to study and to establish reliable statistics ascribed to the lack of reporting by victims, or the difficulty of classifying cybercrime due to the motley forms the scams may take, the diverse websites and chats through which these crimes are committed, and the speed with which cyber criminals develop new methods to commit these crimes.

Focusing on forensic linguistics and following the outline provided by Gibbons (1994), the areas of action of forensic linguistics would focus on three legal aspects. Beginning with the language of the law, which would deal with the language of legal texts, legislations and their interpretation; the language in legal proceedings, which analyses the language produced when arguing the accusations, or the defence; and finally, linguistic evidence in legal proceedings, which refers to the analysis of linguistic

materials at different levels (e.g. phonological-phonetic or lexical-semantic) and their probative value in criminal proceedings. This work will focus on this last point, on how the linguistic analysis of fraud messages will help in certain criminal proceedings or in the development of systems that could provide a better protection against these types of scams.

The objectives of this work are going to deal with testing whether there are certain linguistic features of scam messages, in the direction of providing some kind of linguistic pattern which can be used to identify the scams; and consequently, with the evaluation of the effectiveness of forensic linguistics in catching fraudulent messages.

The goal of this work is to be able to determine some kind of linguistic patterns on deception, or to be able to recognize it through forensic linguistics. This paper is going to address these research questions:

i. What are the most common linguistic features of fraudulent messages?
ii. To what extent can forensic linguistics help users to prevent these types of scams?

Theoretical framework

The authenticity of a text depends on the source of its origin as indicated by Afroz et al. (2012) bearing in mind that the origin of most scams is very unclear or impossible to trace. Forensic linguistics has several tools to establish the authorship of a text, including stylometry, which is based on the comparison of personal characteristics when writing a text, or the writing style of certain social profiles. Thanks to stylometry, literary works have been added to authors whose origin was believed to be unknown, as in the case of Joe Klein (1996) with his work *Primary Colors*, a political novel published under the pseudonym 'Anonymous' which, thanks to the linguistic analysis carried out through stylometry, made it possible to identify its real author. The origin of the fraudulent messages is of great legal use in order to provide a legal response to the crime committed, but the evolution of the different methods used by scammers makes it almost impossible to track them, which is why these forms of crimes are the ones that proliferate to the greatest extent nowadays.

Cyber-scamming is increasing year by year, as the Internet Crime Report (2023) indicates, in just five years the reports will almost double, with a total number in 2019 of 467,361 reports, reaching 880,418 reports in 2023, for a sum of $12.5 billion scammed. These are the official numbers that have been reported to the competent authorities, but it should be noted that there are many cyber-crimes that go unreported. Among the cyber scams, we not only find scams that seek direct monetary gain, but also data theft is quite common, causing even greater personal damage.

Cyber scams can take many different forms, and among the top five varieties of scams reported to official authorities are Technical Support (4.3%), Extortion (5.5%), Non-payment/Non-delivering (5.7%), Personal Data Breach (6.3%), and Phishing (33.9%). As Miranmirkhani et at. (2017) state, in tech support scams, scammers try to convince users that their machines are infected with malware or other technical problems and need their help. Victims are asked to provide the scammers with remote access to their machines, and the scammers obtain personal data to steal money from their personal accounts. Extortions' scams are scams in which the scammer claims to have embarrassing or sensitive information about the victim and threatens to publish it in exchange for money or bank details. Within these scams, we have the so-called Romance Scams, in which the scammers create fake profiles and establish a relationship through which they try to extract money from the victims, who apart from the financial

scam, also get a sentimental one, as Bilz et al. (2023) point out. And related to the Romance Scams are the Sextortions, which are occasionally used as a form of blackmail, as Whitty (2013) claims that the scammers obtain intimate images of the victims, who are then extorted by publishing these images. Non-payment or non-delivering scams are scams in which products are promised for sale but never reach the buyer, or conversely, the scammer buys an item from the victim but never pays for it. Personal Data Breach consists of the theft of personal information and impersonating public entities, or those who hold such data in order to obtain bank details or money. According to Abdelhamid et al. (2014, 1), a phishing scam is "a form of online threat that is defined as the art of impersonating a website of an honest firm aiming to acquire users' private information, such as usernames, passwords, and social security numbers". All of these scams may look fake from the outside, but their effectiveness is reflected in the $12.5 billion that has been illicitly extracted from personal and corporate accounts.

In this paper I am going to focus on the phishing scams and their examination from a linguistic approach, so I am proceeding to analyse the language, not the interface of the messages as such. Based on the linguistics applied to fraudulent messages, there are certain indicators of danger when we receive a message through the network. Scams are created by people, and when writing there are certain linguistic features that can give us clues as to the veracity of the messages that reach us. Also, there are many scams generated by a computer, or through automatic translators, which may not have the optimal language used in legitimate messages, since they are supposed to come from official sources.

Speaking of scams created by a real person on the other side of the screen, scammers regularly employ linguistic cues to create a trustworthy and authentic impression of themselves as mentioned by Adha (2020). Addawood et al. (2019) emphasize that scammers choose third-person pronouns (e.g., we, their, her) over first-person pronouns (e.g., I, me, myself) to distance themselves from the fraudulent message they are conveying. There are very few theoretical references when it comes to the linguistic analysis of scam messages, but many of these messages are visibly false because of the grammatical and spelling errors they contain, as well as numerical symbols and characters interspersed between words, or erroneous verbal correlations. Many of these linguistic characteristics help us understand the lack of veracity of these messages. Not only the linguistic characteristics help us to understand this, but also the generic form of

the salutation suggests that it is not a legitimate medium. Speaking of SMS messages or e-mails, another possible check would be to look at the URL we are asked to click on and verify that the link does not match the institution it claims to be (whether it is a bank, a governmental entity, or a parcel delivery company, for example). In this paper I am going to shed light on this issue and discover if there are other linguistic features that expose scam messages to determine some danger markers when it comes to analysing messages of questionable origin.

Methodology

In this study I am going to conduct a linguistic analysis of 14 scams carried out through SMS messages (8) and e-mails (6). All the scams parsed are aimed at the illegal extraction of money and personal data, posing as banks, parcel delivery companies or other official bodies such as the EDD (Employment Development Department). The focus will be on linguistics and the help it can provide to distinguish legitimate messages from fraudulent messages.

The choice of scams is based on the limited sources provided by the internet, as many of the scams contain personal data and their publication is conditional on the victim's consent. The analysed email scams are taken from a website (https://419scam.org/419money.htm#paulowen) used by Isacenkova et al. (2013). The analysed SMS messages are taken from the internet, as these messages are exposed in a more accessible way for regular internet users.

One of the major limitations I have found when conducting this analysis is that the scams are usually reported to the competent authorities, who protect any publication of them with data protection laws, consequently I have only found one publicly available database on the internet. These scams have very similar characteristics, and the study of the diversity of existing cyber scams is hindered by the fact that only a database is available. Now that online scams are the order of the day, it would be great for investigators if there were more examples of real scams available on the internet, so that the situation could be more widely publicised. Most of the published examples relate to direct financial scams, but there are very prolific scams today that seek monetary gain through less direct means, such as the aforementioned Romance Scams. So, publishing examples of all sorts of scams could help people see new scam patterns being used across the web.

The technique used for the linguistic analysis is first the analysis of the sender, whether it comes from an official or unknown entity. Then, I analyse if the message contains information about the receiver, as they are official messages, they should be personalised. Afterwards, I look at the formal and spelling analysis of the texts, whether the established structure of the emails is well-formulated and whether they contain a good use of punctuation. Once these characteristics have been analysed, which can be a little more visually striking, we can proceed by analysing the linguistic characteristics and whether they contain lexical-grammatical errors. If they were legitimate messages,

the erroneous use of the language would not occur, but scam messages can contain quite a few errors of this type, so we could categorise them as a danger marker. Finally, the type of language use is analysed, (e.g. most of these messages tend to require urgent action, and concise and direct language is quite common).

Results

Within all the linguistic features, it was first analysed whether the message has a sender and whether that sender is known to be an existing entity, since this is one of the main factors on which a text depends to be reliable. As Table 1 shows, 11 of the 14 messages (78.6%) are known to come from a true entity, but in only 6 of those 11 messages (54.5%), the sender claims to be a legitimate entity. This shows that in less than half of the messages the sender is an official entity or claims to be one. This can be one of the biggest indicators of danger when encountering one of these messages, since if the entity that claims to be is fake, the message falls by itself.

Table 1. This table is divided into the different scams analysed, as well as the name of the entity claiming to be and whether the entity is known or invented by the scammers.

Scams	Name of entity	Legitimate or non-legitimate
Scam	UPS	Legitimate
Scam 2	Netflix	Legitimate
Scam 3	Postal Notice	Non-legitimate
Scam 4	UPS	Legitimate
Scam 5	Unknown	
Scam 6	JB Store	Legitimate
Scam 7	Trust Wallet	Legitimate
Scam 8	EDD	Legitimate
Scam 9	Unknown	
Scam 10	Lottery	Non-legitimate
Scam 11	Macsoftware International Lottery BV	Legitimate
Scam 12	Alpha Express	Legitimate
Scam 13	International Lotto / Lottonet	Non-legitimate
Scam 14	orbitalexpress@cooperation.net	Non-legitimate

Table 2 displays the information that the messages contain about the addressee, such as the name or other details. Since these messages claim to be from official entities, they

should have details of the person to whom the message is addressed, and what we can observe is that only 4 of the 14 messages (28.6%) contain information about the recipient. We cannot check whether the personal information contained in these messages is legitimate, as many fraudsters obtain personal data via the Internet. It is also very common for them to use generic names in the messages, given that, as they are messages sent in mass, in many cases the recipient matches the name used in the message. The personification when a message arrives can give us many clues as to whether it is a legitimate message or not.

Table 2. Name and personal information about the receiver of the message.

Scam	Personal information
Scam 1	No
Scam 2	No
Scam 3	No
Scam 4	Name
Scam 5	Name + Lastname
Scam 6	Name
Scam 7	No
Scam 8	Few numbers of credit card
Scam 9	No
Scam 10	No
Scam 11	No
Scam 12	No
Scam 13	No
Scam 14	No

Within the linguistic analysis, punctuation is the next aspect to be analysed. These messages claim to be from official organisations, so their correct spelling should be the norm, but what we observe is that only 4 of the 14 messages do not contain any spelling mistakes, and of these 4 messages only 1 of them is longer than 30 words without counting the links. Among the most common errors found in these messages are the poorly formulated formal mail structures, typographical errors such as double spaces, omission of commas, missing spaces after ‘:’ ‘,’ ‘.’ ‘!’, capital letters in places that do

not correspond, ‘i’ instead of ‘I’ or no capitals after ‘.’. The large number of these errors can already give us a visual clue that the message we have received is a scam.

Table 3 shows the linguistic errors contained in each message, with a total of 9 out of 14 messages having linguistic and grammatical errors; here, as in the analysis of punctuation, the same pattern is repeated: the more words, the more errors. At first glance, these errors may go unnoticed, but the poor readability they produce in the text hinders its comprehension. Among the most common errors that we will find in this category we have the lack of hyphens between compound words, a wrong subject-verb agreement, bad verb conjugations, lack of prepositions, or inappropriate prepositions, wrong singular-plural agreement, bad choice of words, or invented words that do not exist in English. Among other errors we also have the choice of words used in more informal contexts which do not occur in the type of legitimate messages that they try to mimic.

Table 3. Scams with their linguistic errors

Scam	Linguistic error
Scam 1	0
Scam 2	0
Scam 3	0
Scam 4	0
Scam 5	“u” instead of “you”
Scam 6	0
Scam 7	0
Scam 8	“Plugings” instead of “plugins”
Scam 9	“President elect” instead of “president-elect” / “There’s” instead of “there is”
Scam 10	"Be informed that instruments of payment for the sum of £1,500,000.00 to you, is already in our possession" instead of "are already in our possession" / “download” instead of “downloading” / “fill” instead of “fill out” / “certificate” instead of “certificates” / “deducted

	from" instead of "deducted" / "to avoid" instead of "avoid" / "along side" instead of "alongside" / "immediately" instead of "immediately after the" / "effected" instead of "completed" / "24hrs" instead of "24 hours" / "the receipts of" instead of "receiving" / "filled" instead of "filled-out"
Scam 11	"mix up" instead of "mix-up" / "you" instead of "your" / "DEDUCTABLE" instead of "deductible" / "PROCESSMENT" instead of "processing" / "notorisation" instead of "notarization" / "securiry" instead of "security" / "effect" instead of "affect" / "claims" instead of "claims'" / "automaticaly" instead of "automatically" (x2)
Scam 12	"dispatch" instead of "to dispatch" / "hour" instead of "hours" / "you" instead of "you are" / "courier" instead of "to send" / "fourty" instead of "forty"
Scam 13	"is" instead of "are" / "which" instead of "that" / "non resident" instead of "non-resident" / "and" instead of "or the" / "euro" instead of "euros" (x2) / "for" instead of "for the" / "millions" instead of "million" / "the" instead of "its" / "subsections" instead of "subsection" / "deducted from" instead of "deducted" / "Commissions" instead of "Commission" / "want" instead of "like"

Scam 14	“Fri, 5 Aug 2005” instead of “Friday, August 5, 2005” / “that” instead of “for” / “of” instead of “on” / “you” instead of “your” / “informations of “ instead of “information about” / “also” not needed / “Thanks and waiting” instead of “Thanks, I am waiting”

On the other hand, all messages denote a sense of urgency, with a use of direct language, this can be observed especially in the shorter messages, which contain an alarming message followed by a link in which it is assumed they will be able to solve the problem/situation presented in the message. This sense of urgency is also given by the establishment of a time limit to solve the irregular situation given in the message (e.g. ‘Proceed to pay now to avoid delivery delay’, ‘Reactivate it before 24h’, or ‘You are required to... within 4 hours’).

Implications and applications

The results show that using linguistics we can categorise whether a message is a scam or a legitimate one. The different linguistic and spelling errors such as the verbal misuse or the different typographical errors that we have observed in the results of this work are a great danger indicator when analysing these messages. Linguistics is not only of great help to us in the legal field at the time of trial and the analysis of evidence (fraudulent messages), but it is also very useful to us in our daily lives, since the linguistic analysis of these messages can prevent us from avoiding resorting to legal means. It is very important to know the most general linguistic patterns that these types of messages usually constitute, as nowadays anti-Spam software usually categorises most malicious messages as 'spam', although there are messages that always slip through these filters, and these are the ones that increase the high percentage of this type of cybercrime. Therefore, linguistics can be of great help when we encounter one of these messages that has managed to circumvent the software.

In this case, linguistics and linguists are very important when developing these types of anti-Spam software. It is very important to prevent before curing, and if the computer system detects malicious messages more accurately, the percentage of crimes committed through this medium will probably drop. Thus, before turning to forensic linguistics to determine the classification of a message within the legal parameters, we should polish the linguistics within the message classification systems through software, in order to systematically reduce these crimes. But if the fraud has already been committed, greater importance must be given to linguistics within the legal field, since it is what will delimit the different linguistic patterns that these types of messages have followed when defrauding the victim.

Conclusions

The results of the study show the help that linguistics can provide on a personal level in determining the veracity of messages that reach us through the internet. It also reveals how, if the fraud has already taken place, forensic linguistics can determine in court the real meaning of the messages and how they led to the fraud. Despite the findings, the results of the study are limited by the lack of publicly available samples, as they only focus on specific scams, and do not provide the wide range of deception techniques that scammers use online. A greater availability of real-scams examples could be of great use both for their linguistic study and for the knowledge of the population, who are, after all, the ones who are exposed to these scams on a daily basis.

In short, given that forensic linguistics is a relatively new area, and scam messages are a new technique for the fraudulent extraction of data or money, studies in this field could be of great help. Not only could it be of help to Internet users, but also to computer technicians for a more effective implementation of scam detection techniques, and to legal purposes for the determination, through the language used through digital media, of the crime perpetrated.

Works Cited

Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). Phishing detection based associative classification data mining. *Expert Systems Applications, 41(13), 5948-5959.* 10.1016/j.eswa.2014.03.019

Addawood, A., Badawy, A., Lerman, K., & Ferrara, E. (2019). Linguistic cues to deception: Identifying political trolls on social media. *Proceedings of the International AAAI Conference on Web and Social Media, 13*(01), 15-25. https://doi.org/10.1609/icwsm.v13i01.3205

Adha, A. (2020). Linguistic Based Cues in Detecting Deception in Indonesian Language Use. *Argumentum* (1787-3606), (16). https://doi.org/10.34103/argumentum/2020/2

Afroz, S., Brennan, M. & Freenstadt, R. (2012). Detecting hoaxes, frauds, and deception in writing style online. *IEEE Symposium on Security and Privacy,* San Francisco, CA, USA, 461-475. 10.1109/SP.2012.34.

Bilz, A., Shepherd L.A., & Johnson G.I. (2023). Tainted love: A systematic literature review of online romance scam research. *Interacting with Computers*, *35*(6), 773-788. https://doi.org/10.1093/iwc/iwad048

Bossler, A. M., & Berenblum, T. (2019). Introduction: New directions in cybercrime research. *Journal of Crime and Justice, 42(5), 495-499.* https://doi.org/10.1080/0735648X.2019.1692426

Gibbons, J. P. (Ed.). (1994). Language and the Law (1st ed.). *Routledge*. https://doi.org/10.4324/9781315844329

Internet Crime Report (2023). *Department of Justice, Internet Crime Complaint Center, Federal Bureau of Investigation.* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf?trk=public_post_comment-text

Isacenkova, J., Thonnard, O., Costin, A., Balzarotti, D., & Francillon, A. (2013). Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations. *2013 IEEE Security and Privacy Workshops.* doi:10.1109/spw.2013.15

Klein, J. (2006). Primary Colors: A Novel of Politics. *Random House Publishing Group*. 0812976479, 9780812976472

McGuire, M., & Dowling, S. (2013*).* Cybercrime: A review of the evidence. Summary of key findings and implications. *Home Office Research report, 75,* 1-35. https://assets.publishing.service.gov.uk/media/5a74fc06e5274a59fa716800/horr75-summary.pdf

Mellinkoff, D. (2004). *The language of the law*. Wipf and Stock Publishers. 9781592446902.

Miranmirkhani, N., Starov, O., & Nikiforakis, N. (2017). Dial one for scam: A large-scale analysis of technical support scams*. Cryptography and Securit.* https://doi.org/10.48550/arXiv.1607.06891

Starvik, J. (1968). The Evans statements: A Case for forensic linguistics. *University of Gothenburg Press.*

The International Association for Forensic Phonetics and Acoustics (IAFPA). (n.d.). *The International Association for Forensic Phonetics and Acoustics.* https://www.iafpa.net/

The International Journal of Speech, Language and the Law (IJSLL). (n.d.). *International Journal of Speech, Language and Law.* https://journal.equinoxpub.com/IJSLL/index

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *The British Journal of Criminology,* 53(4), 665–684. https://doi.org/10.1093/bjc/azt009

Appendices

1.

FRM:[UPS]

SUBJ:23:50 23/03/2021-Schedule Delivery

MSG:3890007-Sorry, we've missed you. We tried to deliver your parcel today,

(Con't) 2 of 2

http://a2rb4-ups.com/?=426976007

(End)

2.

Netflix: Please update your membership with us to continue watching. bedy13.com/V3n4Ovhcqw

3.

Postal Notice – You have a package that needs to be delivered, but it has been suspended due to an incorrect delivery address. https://uspostinfo.com/Wt4g

4.

UPS. Hi Olivia. Your shipment requires a delivery fee. Proceed to pay now to avoid delivery delay, Visit: https://ups-express.click/?&trck

5.

Hello Amore Onyung, how are u today? hope great. I got your application from indeed regarding the position of Personal Assistant. Kindly click on this link https://goo.gl/0AMaqn read through the requirement and get to me if you are still interested in the position.

Regards.

Alex Garcia.

6.

Dear Leigh! This morning JB Store announced their lottery winners. Congratulations you took 2nd place. Check what you won http://rtapit.com/7FA

7.

Trust Wallet: Your wallet is suspended temporarily. Reactivate it before 24h using tour seed phrase:https://bitly.lc/TrwGE

8.

EDD Alert: You are required to reactivate your EDD Visa Prepaid starting 4427434*** within 4 hours at https://www.roamnana.nl/wp-content/plugings/ioptimization/o.php

9.

Stand up America ! Apply for second face of pandemic stimulus. Biden

signs 1.9 trillion Covid relief bill, clearing way for stimulus checks, vaccine aid. The

President elect is giving $2,400 extra

assistant stimulus to citizens as a relief stimulus package.

there’s

no discrimination, everybody is qualified. Click the link to claim:

https://zfrmz.com/QGWp5tVwiZW3o36oaG5K

10.

Dear Prize Winner,
Acting on the instructions in your claims file with Reference number 3NW-4 and Batch number FN-112, I wish to inform you that payment of your Lottery Claims amounting to £1,500,000.00 being prize money from NATIONWIDE LOTTO UK Third Category draws has been certified by all authorities involved.
Be informed that instruments of payment for the sum of £1,500,000.00 to you, is already in our possession and shall be processed upon meeting the requirements stated below.

You are required to fill a "Lottery Winnings Claim Form" with all necessary details. Follow the link below to download the form

http://www.heritage-finance-ltd.net/lottery.html

After download, kindly print, fill, and send to us either by fax or as an email attachment. You will also be required to pay a fee of £3,670.00 (Three thousand six hundred and Seventy Great Britain Pounds), or its equivalent in your local currency.
This payment is to cover transfer charges, Insurance of vital documents like prize claim certificate and other transfer documents, handling and opening of account charges.
Note that your total prize claim of £1,500,000.00 has been insured to the real value and as such cannot be deducted from. This is in accordance with section 13(1)(n) of the National Lottery Act of the British Lottery Affairs Commission as adopted in 1993 and amended in 1998. This is to protect winners and to avoid misappropriation of funds.

A certificate of prize claim certificate along side other vital documents will be sent to you via Courier service immediately transfer of your winnings is effected.

Note that your winnings will be transferred within 24hrs after the receipt of both requirements stated above.

Congratulations once more, I shall be awaiting your filled Lottery Winnings Claims Form.

Truly yours,

Mr. Dennis Hammond,
Foreign Department Manager,
Heritage Finance Ltd.
Tel: +44-20-7060-0194
Fax: +44-20-7504-3787
EMAIL: dhammond4@heritagefinance-ltd.org
WEBSITE:www.heritage-finance-ltd.net

NB: For further information about NATIONWIDE LOTTO UK, feel free to contact them directly;

NATIONWIDE LOTTO UK
SOUTH PARK BUSINESS CENTRE
310 GREEN LANE, ILFORD,
IG1 1XT, ESSEX.
Phone: +44-70 4010 6614
Fax: +44-20 8181 6406
WEBSITE: www.nationwidelottuk.com

As a winner, you are allowed to login into their website to confirm your winnings.

11.

From: MRS. VERONICA VAN BOSCH [mailto:veronicbosch@netscape.net]

Sent: 27 December 2004 12:50

To: *Full Name*

Subject: CONGRATULATION!!!

MACSOFTWARE INTERNATIONAL LOTTERY BV

Laan Van Hoornwajck 55

2289 Dg Rijswijck

Den Haag, The Netherlands

ATTN:

We are pleased to inform you of the announcement today 27th, December 2004

of winners of the MACSOFTWARE PROMOTION LOTTERY NETHERLANDS /INTERNATIONAL,

PROGRAMS held on 23rd of October 2004. Your email address attached to ticket number 023-56475130154, drew the lucky numbers6-13-11-42-40-59, batch number 6656/NL and consequently won the lottery in the 1st category. You have therefore been approved of a lump sum pay out of (EUR500,OOO:00) FIVE HUNDRED THOUSAND EURO ONLY in credited to file LOTTERY REF NO. SGIL/763276/03. This is from total prize money of EURO 20,000,000.00 shared among the seventeen international winners in categories B with serial number: IL/FLW/12-C033721181.

All participants were selected through a computer ballot system drawn form 25,000 company email addresses and 30,000,000 individual email addresses from Australia,Africa, New Zealand, America, Europe, North America and Asia as part of International Promotions Program, which is conducted annually.

CONGRATULATIONS!

Your fund is now in custody of a financial Security company insured in your FILE REFERENCE. Due to the mix up of some numbers and names, we ask that you keep this award strictly from public notice until yourClaim has been processed and your money remitted to your account.This is part of our security protocol to avoid double claiming or unscrupulous acts by participants of this program. This lottery program was promoted by our group of philanthropist headed by the Netherlands government. We hope with a part of you prize, you Will participate in our end of year high stakes EURO 5,000,000 million International Lottery.

To begin your claim, please contact your file/claim Officer:

MR.WILLIAM ROBINSON
FOREIGN SERVICE MANAGER
STANDARD SECURITY BV
DEN HAAG, THE NETHERLANDS
EMAIL:macsoftlotter@netscape.net
TEL:+31-627-501-802

Please be informed that NON RESIDENCE of THE NTHERLANDS will be required to make a NON DEDUCTABLE advance payment of processment and legal documentation
charges of (EUR928.10 Cent) Nine Hundred And Twenty Eight Euro Ten Cent, to enable our legal department acquire Notorisation papers from the Court prior to award payment policy as required by the paying Financial Securiry Company.Please be aware that your Paying Authority will Effect Payment Swiftly upon satisfactory Report, Verifications and validation provided by our Processing Agent; that would be designated to your file. For due processment and remittance of your winning prize to your designated account of your choice. Remember, all prize money must be claimed not later than 10th of January 2004. After this date, all funds will be returned as unclaimed. NOTE: In order to avoid unnecessary delays and complications, please remember to quote your reference.And batch numbers in every one of your correspondences with your agent. Furthermore, should there be any change of your address, do inform your claims agent as soon as possible. Congratulations once again from our team of staff and thank you for being part of our promotional program. Note: Anybody under the age of 18 is AUTOMATICALY DISQUALIFIED.

And batch numbers in every one of your correspondences with your agent. Furthermore, should there be any change of your address, do inform your claims agent as soon as possible. Congratulations once again from our team of staff and thank you for being part of our promotional program. Note: Anybody under the age of 18 is AUTOMATICALYDISQUALIFIED.

Yours sincerely,
Mrs.Veronica Van Bosch
Lottery Coordinator

12.

Dear customer,

Good day to you. This is to inform you that we are in possession of certain documents and certified cheques which are to be couriered to you. You are to please confirm your mailing address to enable us dispatch your parcel immediately.

Note that we also do not deliver to P.O.Box address or street corners but to your residence. We are a well established company offering courier and transport services 24 hour a day for priority delivery of letters, parcels and consignments to any destination. Alpha Express Deliveries with its high security storage and network of affiliate security partners and agents around the world provide you with storage and specialized courier services through which you could send high quality goods like precious stones, art crafts and classified commodities to any part of the world.

Your Parcel number is AEX97451. Description of parcel to be delivered:

An original certificate of weight :----------0.15kg
Bonded draft of weight :----------0.17kg
Total weight of parcel :----------0.32kg
Colour of Parcel :----------Brown

Delivery Destination:
Name: *Firsname lastname*
Address: Not confirmed

We do not operate on COD. Below are the mandatory administrative charges that you required to pay to enable us courier your certificate of winnings

as well as your certified bank cheques to you:

Courier charges.....75.00 Pounds
Administrative .....110.00 Pounds
Insurance ..... 220.00 Pounds
TOTAL 405.00 Pounds (785.40USDollars)

The charges are a little high because of the insurance cover we have undertaken incase of loss, damage or theft of your highly sensitive document before it gets to you. We assume all responsibilities incase of any eventualities.

You are to make the payment through Money Gram money Transfer so as to speed up the process of delivery. You are to locate the nearest money gram agent to you and make the payment in the name of our accounts officer below:

Mr Lawrence Yolelo
3-4 Abbey Orchard Street, Westminster, SW1P 2JJ

You are to fax this office a copy of the transfer slip. If you do not have a fax machine, just send the following information via email as they appear on the money gram transfer slip:

1.Name and address of sender
2.Amount sent
3.Reference number

You are to send a copy of the evidence of payment to your handling agent as well for confirmation. A receipt of the above payment will be couriered to you from our office, along with your winning cheques and certificate.

As soon as we receive confirmation of your address and evidence of payment of the above charges, we will dispatch your documents immediately. The date and time of departure and expected date of delivery will be sent to you. It will take less than fourty eight hours to get your document to you. You will be required to sign for the parcel personally. You will be required to present a copy of your international passport or your driver's license as identification.

All orders not delivered within Five(5) working days from this communication will be returned as unclaimed.

We are glad to be of service to you.

Mr John Walters
Customer service
Alpha Express delivery services
3-4 Abbey Orchard Street, Westminster, SW1P 2JJ
Phone:+44-207-060-0353
Fax :+44-870-831-0812

==========

==========

Tel: +(44) 2070600353 . All business is transacted under our Standard

Trading Terms and Conditions a copy of which is available upon request . All

liability for viruses is excluded to the fullest extent permitted by law

There's the network for sending IP address 80.179.242.243:
Gilat / Golden Lines is a satellite internet service provider for Nigeria and other West African countries.

inetnum: 80.179.242.224 - 80.179.242.255

netname: Gilat-ART2036

descr: Please Send Abuse/SPAM complaints To Abuse-gilat@012.net.il

country: GB

admin-c: DR5299-RIPE

tech-c: DR5299-RIPE

status: ASSIGNED PA

notify: lir@linux.goldenlines.net.il

changed: lir@linux.goldenlines.net.il 20040617

mnt-by: AS9116-MNT

mnt-lower: AS9116-MNT

source: RIPE

route: 80.179.128.0/17

descr: Golden Lines

origin: AS9116

mnt-by: AS9116-MNT

changed: lir@linux.goldenlines.net.il 20020711

source: RIPE

role: DNS REG

address: 25 Hsivim st. Petach-Tiikva, Israel

e-mail: dnsreg@012.net.il

trouble: abuse@012.net.il

admin-c: GE2074-RIPE

tech-c: IB737-RIPE

tech-c: AG914-RIPE

nic-hdl: DR5299-RIPE

notify: lir@linux.goldenlines.net.il

changed: lir@linux.goldenlines.net.il 20030715

mnt-by: AS9116-MNT

source: RIPE

13.

From: "Michael Moses" <michaelmoses_lottonet@yahoo.co.uk>
To: <*emailaddress*>
Sent: Sunday, 30 January, 2005 6:09
Subject: Your ref: 014/061/500

Attn: *Firstname Lastname*,

INTERNATIONAL LOTTO

Our ref: OAM/024/63WD/03

Your ref: 014/061/500

Branch office: 400 Clontarf rd
Dublin 3
Dublin - Ireland.
Email address: michaelmoses_lottonet@yahoo.co.uk

RE: CLAIM OF LOTTERY JACKPOT

We are happy to inform you that the confirmation and investigation process is now complete. We have no problem with the information you declared in the Application form which you filled and submitted to this office.

As has been observed from the said application for payment form submitted to our offices, you are a non resident of Ireland and United Kingdom. As such, a certificate of clearance from the Court here would be required and must therefore be processed by this office on your behalf.

In this light you are immediately required to pay a fee of €2010 (Two thousand and ten euro), or its equivalent in your local currency.

This payment is for items stated below:
1) Endorsement Fee of €960.00
2) Affidavits of lotto claim/Court clearance
certificate of Clearance fee of €1050.00

Grand Total of €2010 (Two thousand and ten euro).

Note that your total prize claim of €2,000,000.00 (Two millions euros) has been insured to the real value and as such cannot be deducted from. This is in accordance with article 44 subsections 144 of the International Lottery Commissions gaming regulations as amended in the 1996 constitution. This is to protect clients (WINNERS) and to avoid misappropriation of funds. Please note that without the payment of the Endorsement Fee, affidavits of lotto claims and the certificate of clearance fees, your claim cannot be completely processed.

As soon as you indicate your readiness to send the requested fee to us, we shall advise you of the proper and fastest means to get the money to us.

Note: Kindly let us know how you would want to receive your money. This shall be processed by our bank. We do not disclose information of paying bank to avoid false claim.

Please revert

With Friendly Greetings,

MICHAEL MOSES
LOTTONET
400 Clontarf RD
Dublin 3
Dublin - Ireland
Tel: +447040103703
Fax: +448701334013
Email: michaelmoses_lottonet@yahoo.co.uk

Asking "whois.ripe.net" about "83.170.12.18":

inetnum: 83.170.12.0 - 83.170.13.255

netname: DE-IABG-TELEPORT-COBRANET-ISP

descr: IABG - Teleport customer CobraNet

country: LB

admin-c: HM1517-RIPE

tech-c: ED740-RIPE

status: ASSIGNED PA

notify: guardian@teleport-iabg.de

mnt-by: IABG-MNT

changed: gabriel@iabg.de 20040616

source: RIPE

route: 83.170.0.0/18

descr: IABG mbH

origin: AS29259

notify: lir.teleport@iabg.de

mnt-lower: IABG-MNT

mnt-routes: IABG-MNT

mnt-by: IABG-MNT

changed: bschmidt@teleport-iabg.de 20040420

source: RIPE

person: Hikmat Mardo

address: Lagos-Nigeria

address: Lekki Phase 1

address: rafiu babatunde street plot 8

phone: +23417767720

phone: +234802 832 2133

phone: +23415555656

phone: +9613666325

e-mail: hjm@cobranet.org

nic-hdl: HM1517-RIPE

notify: guardian@teleport-iabg.de

mnt-by: IABG-MNT

changed: gabriel@iabg.de 20040617

source: RIPE

person: Elie Dib

address: Lagos-Nigeria

address: Lekki Phase 1

address: rafiu babatunde street plot 8

phone: +9613235266

e-mail: elie@cobranet.org

nic-hdl: ED740-RIPE

notify: guardian@teleport-iabg.de

mnt-by: IABG-MNT

changed: gabriel@iabg.de 20040617

source: RIPE

14.

From: orbitalxpress@cooperation.net
To: *Firstname Lastname <emailaddress>*
Subject: way of helping you pay for the charges
Date: Fri, 5 Aug 2005 17:50:56 +0200
Dear winner,

How are you doing today? Well,i am writing to inform you that there has been a recent development since the last time you wrote.The inland tax revenue has asked that a tax of out of country winnings of 1% of your winnings be paid by you before you funds can be delivered.Knowing fully well that you were unable to raise the required fees needed to deliver your winnings,i have contacted a financier who has promised to assist you pay up these charges for 5% of your winnings .He promised that he was going to issue you the money but if you could provide some certain informations of your credit card so that he could be able to load the amount needed into it and help save this predicament.

Due to his location now (he is on a new exploration site and far out of town), he's unable to do anything towards that effect, so he is left

with no other option, but to send you the funds, through your credit card(s).

So, please send me the following details, as these are the only details he would require to send the money, faster and more convininetly to you through the credit card account you will provide:

1. Name of Issuing Bank
2. Payment center address and tel. number (found on the monthly statement)
3. 16 digit card number
4. Credit Card limit
5. Available balance (amount owing)

Please note, that the above information required of your credit card, does not jeopardise your card security in anyway, as sensitive details such as your Social Security Number, Date of Birth, CVC, Expiry date and others,are not required to make payments into it.

Upon receipt of your card payment information, the financier will load it accordingly and you can empty it and he will continually have it re-loaded, depending on the credit limit of your card, also let me know the exact amount you require to make your claims.
So that I will know in what installments i will upload the credit card.

Thanks and waiting on your information
CharlesDenovan
~~~~~~
~~~~~~