sciendo

Land Forces Academy Review
Vol. XXX, No. 2(118), 2025

OLDIE BUT GOLDIE – USING "TROPES" SOFTWARE TO EXTRACT PHISHING SEMANTIC FEATURES

Radu MOINESCU
"Ferdinand I" Military Technical Academy, Bucharest, Romania
radu.moinescu@gmail.com

Ciprian RĂCUCIU
"Ferdinand I" Military Technical Academy, Bucharest, Romania
ciprian.racuciu@gmail.com

Carmen-Silvia OPRINA
"Ferdinand I" Military Technical Academy, Bucharest, Romania
carmenoprina@yahoo.com

ABSTRACT

Phishing detection remains a critical challenge due to the evolving nature of social engineering tactics. This study leverages "Tropes" software to extract semantic features from phishing messages, utilizing linguistic and contextual analysis to enhance classification accuracy. By identifying recurring patterns and deceptive language structures, our approach improves phishing detection beyond traditional keyword-based methods. This research highlights the effectiveness of linguistic-based phishing classification and underscores the potential of semantic feature extraction in strengthening cybersecurity defenses against increasingly sophisticated phishing attacks.

KEYWORDS: social engineering, deceptive language, semantic analysis, phishing detection

1. Introduction

Phishing remains one of the most common methods by which cybercriminals target their victims. In this context, identifying and extracting specific phishing features becomes essential for developing effective defense solutions. This article aims to explore the use of the "Tropes" software (Tropes, n.d.) as a tool in the analysis and extraction of features associated with phishing attacks.

Developed by Pierre Molette and Agnès Landré, based on the research of Rodolphe Ghiglione, "Tropes" is an advanced software for automatic text analysis, useful for both researchers and professionals in various fields, such as linguistics, sociology, speech psychology and communication sciences. This tool has a complex set of functionalities that facilitate a deep semantic approach, allowing the exploration and understanding of discourse by highlighting relationships, actors and central themes in texts (Molette, 2009). Even though "Tropes" may seem an outdated software, its application in the field of cybersecurity highlights the value of traditional solutions, demonstrating that they

DOI: 10.2478/raft-2025-0027

can provide valuable insights in protecting users from online threats. This approach has the potential to transform the understanding and combating of phishing in the context of the contemporary digital landscape.

2. Related Work

The detection of phishing attacks has been extensively studied, with numerous approaches leveraging machine learning (ML), natural language processing (NLP), and semantic analysis to enhance phishing classification accuracy.

Gastón L'Huillier et al. (2010) explored the use of latent semantic analysis (LSA) and keyword extraction for phishing classification. Their method focuses on identifying key phrases in phishing e-mails by analyzing the latent semantic structure of the e-mail content. The authors proposed that these techniques can improve phishing detection by capturing semantic relationships that traditional keyword-based approaches may overlook.

In a later study, Xi Zhang et al. (2017) advanced phishing detection by integrating semantic analysis with boosting algorithms. By combining these techniques, they aimed to enhance the phishing detection performance, demonstrating that semantic-based features could significantly improve classification accuracy compared to standard methods. The research highlighted the importance of extracting deeper semantic insights from phishing e-mails for more robust detection.

Sikha Bagui et al. (2019) focused on utilizing both ML and deep learning (DL) approaches to classify phishing e-mails. Their study compared various algorithms, including traditional ML models like Support Vector Machine (SVM) and decision trees, with DL techniques. The authors found that DL models, particularly neural networks, outperformed conventional methods in accurately classifying phishing e-mails, showcasing the potential of these techniques in detecting sophisticated phishing attacks.

Gilchan Park and Julia M. Taylor (2021) proposed a text-based phishing detection system that leverages NLP techniques for more accurate classification. Their work emphasized the importance of contextual analysis of the e-mail text, aiming to understand not only the individual words but also the relationship between them. By focusing on text-specific features, the authors demonstrated a promising direction for detecting phishing attempts embedded within natural language.

Said A. Salloum et al. (2022) conducted a systematic literature review on phishing e-mail detection using NLP techniques. The review covered a wide range of methods employed in this domain, categorizing approaches into feature extraction, classification techniques, and evaluation metrics. The authors found that while NLP-based methods have shown significant progress, there is still a need for more robust models that can handle diverse phishing strategies, especially with the evolving tactics used by attackers.

Together, these studies highlight the evolving nature of phishing detection, with a shift towards more sophisticated semantic and text-based analysis combined with ML and DL models. However, challenges remain, particularly in dealing with the dynamic and increasingly deceptive strategies employed in phishing attacks.

3. Features of the "Tropes" Software Useful for Identifying Phishing

"Tropes" is distinguished by its ability to perform a thorough analysis of the text content, focusing on the following key aspects:

– *Vocabulary analysis*: "Tropes" can identify words and phrases commonly used in phishing e-mails, such as "*account locked*", "*personal information*", "*account verification*", or "*urgent*". It can also detect misspelled or misspelled words, which are often present in phishing messages;

– *Syntactic structure analysis*: "Tropes" can analyze the grammatical structure of the text and identify unusual or erroneous constructions that may suggest a phishing message. For example, phishing messages may contain short, imperative sentences designed to create a sense of urgency;

– *Thematic analysis*: "Tropes" can identify the main themes of the text and highlight topics that are commonly associated with phishing, such as security issues, fake offers, or requests for personal information;

– *Emotional analysis*: "Tropes" can analyze the emotional tone of the text and identify messages that convey a sense of urgency, fear or exaggerated excitement, which are often used in phishing to manipulate the victim;

– *Morphological ambiguity handling*: "Tropes" can decide between the different meanings of a word, such as between a verb and a noun or between a noun and an adjective. This operation is based on a language-specific syntactic matrix, local grammar, context and disambiguation rules written by lexicographers.

4. Extracting Phishing-Specific Semantic Features with "Tropes"

This study examines the semantic characteristics of phishing attacks by analyzing a corpus of 4,000 phishing e-mails (https://monkey.org/~jose/phishing/) collected by researcher Jose Nazaio between 2015, and 2024. The analysis focused exclusively on the textual content, specifically the header (e-mail Subject) and the message body, while excluding sender addresses. This approach enabled a detailed investigation of the linguistic strategies employed in phishing e-mails, independent of sender-specific metadata. To ensure consistency in analysis, only English-language e-mails were included in the dataset.

This dataset, a resource often used in scientific research, was selected for analysis due to its size, time span covered, and public availability, thus ensuring the accessibility and reproducibility of the study.

The analysis was conducted using the "Tropes" framework. By examining these patterns, the study highlights the specific linguistic techniques that contribute to the persuasiveness and effectiveness of phishing attacks.

People's psychological state is directly influenced by the words they read, which have the ability to generate specific emotional and behavioral reactions. This principle is successfully exploited in phishing e-mails. Attackers do not limit themselves to technical vulnerabilities, but directly target the psychological weaknesses of the recipient, using instinctive reactions and mental traps to mislead them.

The header of a phishing e-mail, especially the "*Subject*" field, plays a key role in grabbing the recipient's attention and inducing a quick reaction. By exploiting specific psychological factors, attackers use a set of keywords and linguistic constructs designed to trigger emotions and impulses that increase the likelihood that the victim will open the message and follow its instructions.

In our study, we developed a linguistic taxonomy of phishing attacks, classifying e-mails according to the psychological vulnerability or emotion exploited. This classification allowed us to identify recurring keywords associated with each category, providing detailed insight into the linguistic strategies used by attackers.

Phishing categories and related keywords (Figure no. 1):

– *Helpfulness*: This category targets the feeling of altruism and the desire to help. Commonly used keywords include: donation, help, humanitarian, charity, support, victims, crisis, refugees, volunteer, hospital;

– *Sexual attraction*: Attackers exploit the desire for romantic or sexual connection. Typical keywords include: date, flirt, love, romantic, private messages, profile, admirer, relationship, connection, passionate;

– *Convenience*: This category is based on the promise of quick and easy gain.

Relevant keywords include: easy, fast, automatic, effortless, simple, instant, accessible, convenient, free, simplified;

– *Compassion*: Attackers appeal to the empathy and compassion of victims. Commonly used keywords include: suffering, empathy, care, help, sadness, tears, child, helpless, treatment, hope;

– *Gullibility*: This category exploits the naivety and gullibility of victims. Typical keywords are: congratulations, winner, prize, selected, special, free, exclusive, lucky, surprise, bonus;

– *Curiosity*: Attackers use language to arouse the curiosity and interest of victims. Relevant keywords include: secret, shocking, reveal, mystery, you won't believe, surprise, news, details, see now, secret information;

– *Fear*: This category relies on inducing fear and a sense of urgency. Commonly used keywords are: alert, danger, problem, fraud, suspended, attack, compromise, threat, deception, hacking;

– *Greed*: Attackers exploit greed and the desire to make a quick buck. Typical keywords are: gain, money, profit, opportunity, discount, deal, millions, wealth, return, investment;

– *Respect/fear of authority*: This category is based on intimidating victims by invoking authority. Relevant keywords include: bank, official, notice, police, government, lawyer, document, legal, account, restriction;

– *Sense of urgency*: Attackers create a sense of urgency to cause victims to act impulsively. Commonly used keywords are: urgent, immediate, limited time, expire, act now, last chance, today only, hurry, low availability, critical;

– *Sympathy*: This category is based on building a relationship of trust and sympathy with the victim. Typical keywords are: friend, family, special message, kind thoughts, you care, relationship, connection, closeness, emotional, sincerity;

– *Vanity*: Attackers exploit victims' vanity and desire for recognition. Relevant keywords include: VIP, exclusive, premium, honor, recognition, distinction, chosen, unique, renowned, prestigious.

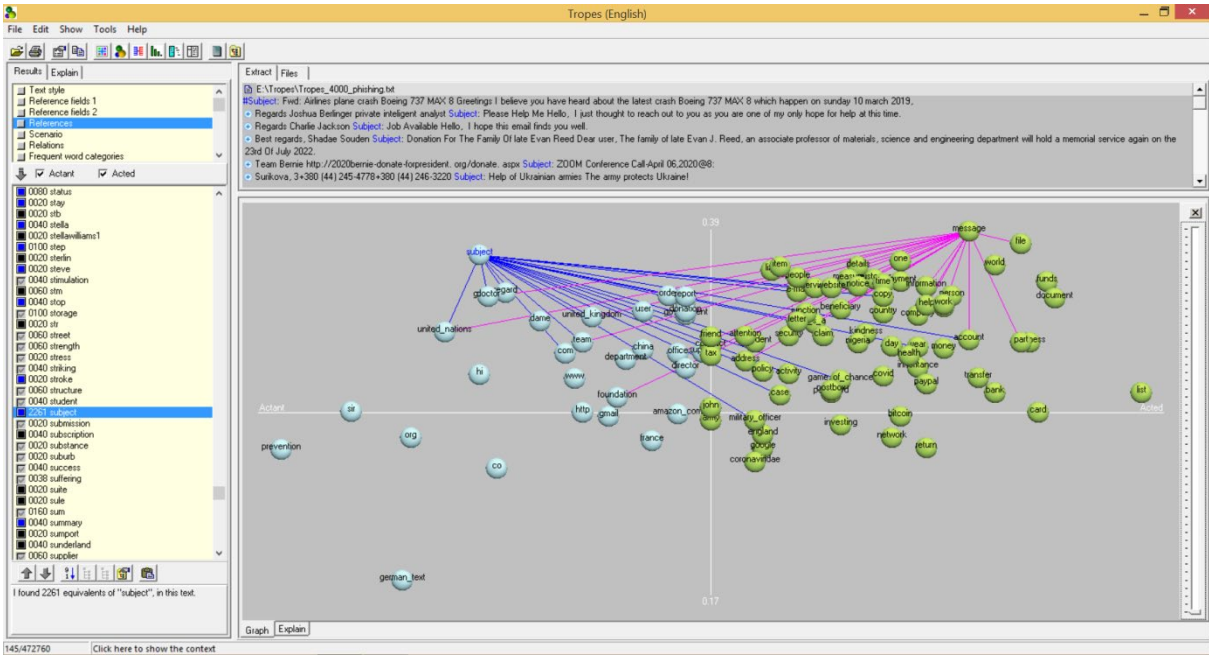

Figure no. 1: *Some of the keywords used in phishing e-mail "Subjects" identified by "Tropes"*
(Source: Authors' creation)

After analyzing the corpus of 4,000 phishing e-mails, we developed a statistic of the frequency of each category, providing insight into the most exploited psychological vulnerabilities. This statistic is presented in Table no. 1.

In analyzing phishing e-mails, not only the keywords in the "*Subject*" field play a crucial role, but also the semantic constructions in the body of the message. The sentences and phrases used in phishing messages are designed to stimulate strong emotional reactions and impulses that prevent the recipient from thinking critically or questioning the legitimacy of the message. Thus, by manipulating language and using a set of semantic constructions, attackers create contexts that lead to a quick and often unjustified decision on the part of the victim. Next, we will analyze how semantic constructions align with the emotional and psychological categories mentioned above.

Table no. 1

Statistical distribution of keywords in the header of phishing e-mails

Exploited category:	Frequency:
Helpfulness	2.44%
Sexual attraction	1.22%
Convenience	3.66%
Compassion	1.22%
Gullibility	12.20%
Curiosity	9.76%
Fear	29.27%
Greed	19.51%
Respect/fear of authority	4.88%
Sense of urgency	14.63%
Sympathy	0.61%
Vanity	0.60%

(Source: Authors' creation)

Semantic constructions that evoke *helpfulness* are strategically formulated to create a dramatic or urgent scenario, appealing to the recipient's altruism. These constructions are designed to manipulate the victim's emotions, prompting immediate action without critical evaluation:

– *"The refugee crisis in [region] has reached a critical point. Your financial contribution can provide shelter and food for those displaced"* (specificity, appeal to basic needs, emotional impact);

– *"The [name] hospital is short of essential medicines. A donation, no matter how small, can save lives"* (specificity, emotional impact, emphasis on the importance of each donation).

Such formulations often emphasize **clarity** and **specificity**, ensuring that the message is easily understood while providing concrete details to enhance credibility. Additionally, they incorporate **emotional impact**, leveraging sentiments such as compassion, urgency, and solidarity to increase persuasive effectiveness.

Further, phishing messages frequently appeal to **basic human needs**, such as food, shelter, and medical assistance, reinforcing the necessity of immediate intervention. By focusing on **vulnerability** – especially that of children or disaster victims – these messages intensify the emotional response. Calls to **immediate action** and **solidarity** further heighten the pressure on the recipient,

framing the requested contribution as both urgent and morally imperative.

The strategic use of factive verbs (Figure no. 2) in the semantic constructions of phishing e-mails, which evoke the feeling of helpfulness, contributes to the illusory validation of dramatic scenarios, thus amplifying persuasion and diminishing the recipient's critical evaluation.

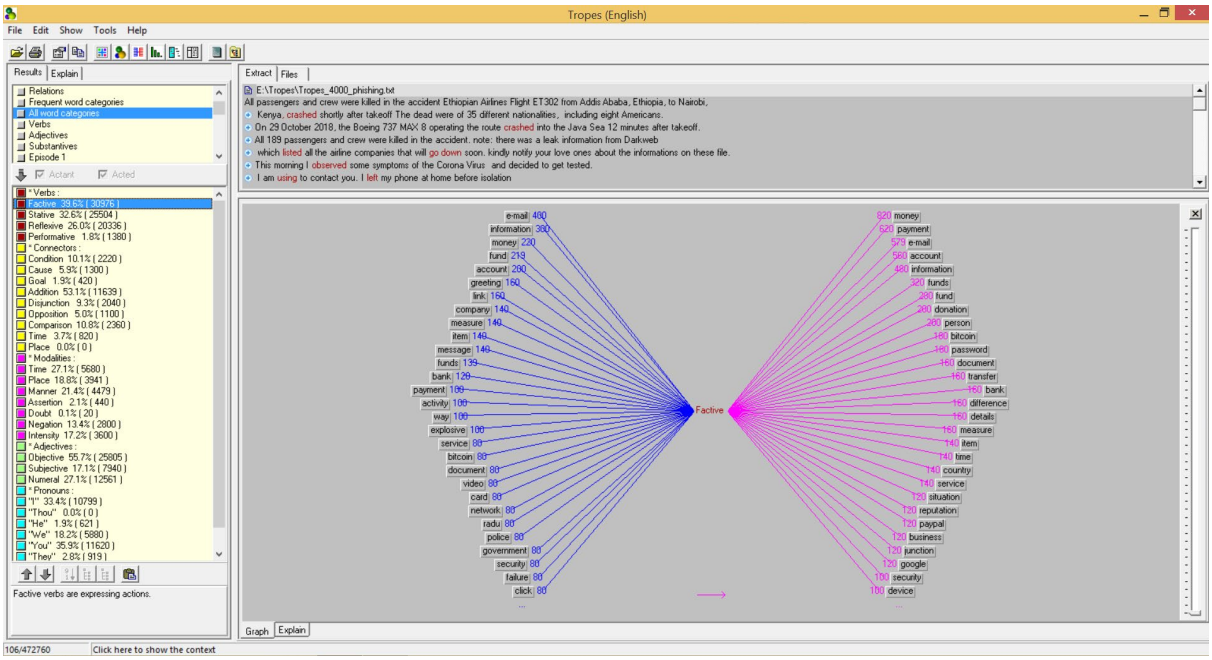

Figure no. 2: *Some factives from phishing e-mails identified by "Tropes"*
(Source: Authors' creation)

In *sexual attraction* phishing attacks, semantic constructs are deliberately designed to evoke a sense of **personal connection** and **romantic or sexual interest**. These messages exploit the **emotional vulnerability** of potential victims by simulating the dynamics of genuine romantic interactions, increasing the likelihood of engagement:

– *"I feel an inexplicable attraction to you. I would be honored to get to know you better"* (expressing an attraction, mentioning an inexplicable feeling, proposing a deeper acquaintance);

– *"I imagine a special connection between us. Are you willing to discover if I'm right?*" (suggestion of a special connection, invitation to discovery).

A common strategy involves employing a **respectful and personalized approach**, where messages reference specific details about the recipient to create a sense of authenticity. Additionally, **flattery** is frequently used to enhance the victim's self-esteem, making them more receptive to further interaction. By emphasizing **intrigue** and **curiosity**, attackers stimulate interest while maintaining an air of mystery, prompting the victim to seek more information.

Moreover, these messages often **avoid pressure** by subtly suggesting an initial dialogue rather than demanding immediate action. This measured approach fosters a sense of control in the recipient, reducing suspicion. The **promise of a deep emotional or intellectual connection** further reinforces engagement, as messages highlight shared values, unique experiences, or rare compatibility.

In *convenience* phishing attacks, attackers exploit the victim's preference for efficiency and minimal effort by crafting messages that promise **quick**, **effortless solutions**. These messages are designed to reduce skepticism by emphasizing **simplicity**,

automation, and **immediacy**, making the proposed action appear both appealing and risk-free:

– *"Unlock [benefit] instantly, without any effort. Everything is configured for you"* (instantaneousness, effortlessness, personalization);

– *"Don't waste precious time. [solution] gives you [benefit] instantly and without any effort"* (time saving, specific solution, instant benefit, lack of effort).

A key linguistic strategy involves **clarity** and **specificity**, ensuring that the promised benefit is well-defined and easily understood. By presenting the solution as **exclusive** or **time-sensitive**, attackers create a sense of urgency, increasing the likelihood of immediate action. Additionally, the **lack of required effort** is a recurrent theme, reinforcing the idea that the victim can obtain the advertised advantage with minimal involvement.

Furthermore, messages frequently incorporate **calls to action**, using imperative verbs to encourage recipients to engage immediately. The promise of **instantaneous results** and **automation** further strengthens persuasion, as victims are led to believe that no additional steps or decisions are necessary.

In phishing attacks that exploit *compassion*, semantic constructions are strategically designed to evoke **empathy** and **moral responsibility**, persuading victims that their assistance can have a tangible impact. These messages manipulate the recipient's emotions by emphasizing **human suffering**, reinforcing the idea that inaction would result in continued distress for vulnerable individuals:

– *"Children affected by the conflict in [region] are in desperate need of support. A donation, no matter the amount, can provide a future for these children"* (specificity, emotional impact, appeal to hope);

– *"Your care can bring comfort and hope to the souls of those who feel abandoned and helpless"* (emotional impact, appeal to care, emphasis on the importance of help);

A common linguistic technique involves **specificity**, were messages reference particular crises, affected groups, or essential needs such as food, shelter, or medical aid. This approach enhances **credibility** and makes the appeal more compelling. Additionally, **emotional impact** is a central element, leveraging **compassion**, **urgency**, and **moral obligation** to elicit an immediate response. By portraying the victim as a potential **hero** or **lifeline** for those in distress, attackers further intensify the psychological pressure to act.

Another prevalent strategy is the **call to action**, which frames the donation or contribution as a **direct** and **immediate solution** to the problem. Phrases emphasizing **solidarity** and **collective responsibility** reinforce the notion that the recipient's support is both necessary and expected.

In phishing attacks that exploit *gullibility*, attackers craft messages that create a **false sense of trust** and **urgency**, appealing to the victim's **naivety** and **desire for effortless rewards**. These messages often leverage psychological triggers such as **exclusivity**, **guaranteed success**, and **time-sensitive opportunities** to manipulate recipients into taking immediate action:

– *"You have the opportunity to win [amount] without any effort. All you have to do is fill out a short survey"* (specific amount, no effort, specific action);

– *"Don't miss this unique opportunity to become a millionaire! Sign up now and you have the chance to win [amount]"* (uniqueness, specific amount, call to action).

One common strategy involves **specificity**, where messages mention a concrete prize, amount, or benefit to enhance credibility. By incorporating **clear instructions**, attackers simplify the required action, making it seem straightforward and risk-free. Additionally, the use of **urgency** pressures the victim into responding quickly, reducing the likelihood of critical evaluation.

Another key element is the **call to action**, often framed as an immediate and

effortless process to claim a reward. Attackers frequently **downplay risks** while emphasizing **guaranteed benefits**, reinforcing the idea that the victim stands to gain without any real effort. However, these messages often contain **privacy risks**, subtly requesting personal details under the pretense of prize redemption.

In phishing attacks that exploit *curiosity*, attackers craft messages that leverage the recipient's **desire for exclusive or sensational information**, prompting them to engage without skepticism. These messages often utilize **attention-grabbing headlines** and **emotionally charged language**, making the content difficult to ignore:

– *"Discover a shocking secret about [topic of interest]. The truth will surprise you!"* (specificity, emotional impact, promise of revelation);

– *"You won't believe what we've learned about you! Open this message to learn more"* (emotional impact, personalization, call to action).

A key strategy involves **specificity**, were attackers' reference particular **topics**, **individuals**, or **organizations**, increasing the perceived credibility of the claim. Additionally, **emotional impact** is employed through words that evoke **shock**, **mystery**, or **urgency**, compelling recipients to seek further information.

Another common tactic is the **promise of revelation**, which suggests that the recipient is on the verge of uncovering **hidden** or **suppressed knowledge**. This is frequently combined with **urgency**, implying that the information is only available for a limited time, encouraging immediate action.

The **call to action** is central to these messages, directing the recipient to follow a link, open an attachment, or provide credentials to access the supposed revelation.

In phishing attacks that exploit *fear*, attackers craft messages designed to **induce anxiety and urgency**, compelling recipients to act impulsively without critically assessing the situation. These messages often rely on **formal or technical language**, which enhances credibility and makes the threat appear legitimate:

– *"We have detected an attempt to gain unauthorized access to your account. Please update your password urgently"* (specific, technical language, call to action);

– *"Your personal information may be at risk of security breach. Please review and update your contact information"* (impersonal language, avoid panic, call to action);

A key linguistic strategy is **specificity**, where references to particular **accounts**, **transactions**, or **security breaches** create a sense of realism, increasing the likelihood of user engagement. Additionally, **impersonal language** is frequently used to maintain an authoritative tone while avoiding excessive alarm, ensuring that the victim perceives the threat as serious but manageable.

The **call to action** plays a crucial role, instructing recipients to **review**, **update**, or **verify** their credentials to resolve the alleged issue. Often, this is paired with **clear instructions**, making it easy for victims to comply without hesitation. Some messages employ **precautionary language**, recommending security measures such as updating passwords or monitoring account activity, further reinforcing the illusion of legitimacy.

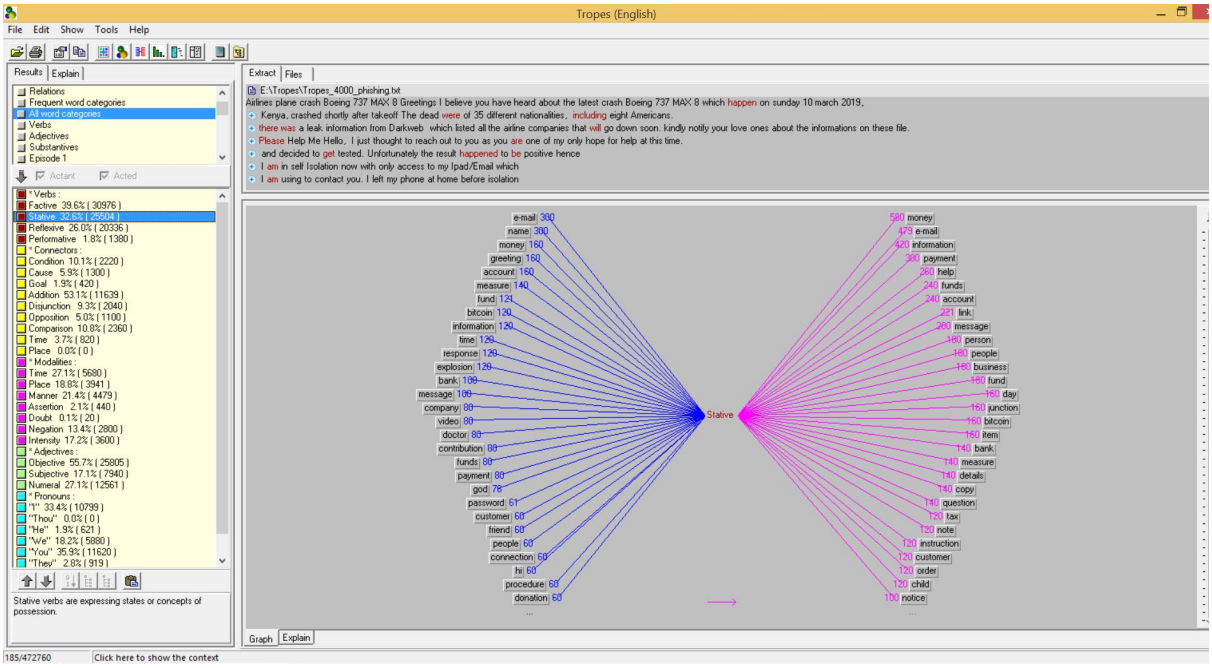

Figure no. 3: *Some statives from phishing e-mails identified by "Tropes"*
(Source: Authors' creation)

The strategic use of **stative verbs** (Figure no. 3) in phishing e-mails, which evoke fear, serves to amplify the sense of vulnerability and urgency among recipients, thus facilitating emotional manipulation and increasing the likelihood of impulsive reaction.

In phishing attacks that exploit *greed*, attackers construct messages that **promise substantial financial rewards with minimal effort**, leveraging the victim's desire for rapid and effortless wealth accumulation. These deceptive communications frequently employ **professional and persuasive language** to enhance credibility, making the offer appear legitimate and enticing:

– *"You have a unique opportunity to become a millionaire! Take advantage of this exclusive offer and turn your savings into a fortune"* (uniqueness, exclusivity, transformation of savings);

– *"We offer a 100% return on your investment! Do not miss this opportunity to multiply your capital quickly and safely"* (specific return, speed, safety);

One key linguistic technique is **specificity**, where precise figures, investment opportunities, or financial instruments are mentioned to create an illusion of authenticity. Additionally, **risk minimization** is a common strategy, assuring the recipient that the investment carries **low** or **no risk**, thereby reducing skepticism. The **promise of exponential growth** or **guaranteed returns** further reinforces the urgency of participation, often paired with **time-sensitive phrasing**, such as "*limited offer*" or "*act now*", to pressure the victim into making an immediate decision.

Another critical element is the **use of exclusivity**, where the message conveys that the opportunity is available only to a select few, increasing the perceived value of the offer. Similarly, references to **financial transformation**, such as turning modest savings into a fortune, appeal to individuals seeking economic security or wealth.

In phishing attacks that exploit *respect/fear for authority*, attackers use semantic constructions that manipulate the victim's sense of obligation and respect for

powerful institutions or individuals. These constructions aim to instill a sense of urgency and submission, often by invoking formal and authoritative language to create the illusion of legitimacy:

– *"If you do not comply with our request, you will be sanctioned according to the legal provisions. We urge you to act promptly"* (legal consequences, call to action);

– *"In accordance with a request from the competent authorities, please provide the requested information within [deadline]"* (official request, deadline);

A common tactic involves the **use of specificity**, where precise dates, deadlines, or official references (such as notification numbers or legal provisions) are presented to lend authenticity to the message. This specificity is intended to mimic the formal communication style of institutions, thereby enhancing the perception of credibility. Additionally, the **official nature** of the message is emphasized through language that references policies, regulations, or legal obligations, reinforcing the idea that the victim is under the authority of a higher power.

The **call to action** is another critical component in these phishing attempts, where the victim is instructed to take immediate steps to comply with what is framed as an urgent request. This is often paired with the threat of **consequences**, such as account suspension or legal sanctions, should the victim fail to comply. Such tactics exploit the victim's fear of legal or financial repercussions.

In phishing attacks that exploit the *sense of urgency*, attackers strategically employ semantic constructs designed to pressure victims into making quick decisions by presenting the illusion of an imminent loss or expiring opportunity. These tactics aim to provoke an immediate response, capitalizing on the victim's fear of missing out or suffering negative consequences:

– *"Last chance to purchase [product] at a discounted price! Hurry, offer expires soon!*" (last chance, discounted price, urgency);

– *"This unique opportunity to [benefit] closes in a few minutes! Don't miss this chance!*" (specific benefit, uniqueness, urgency).

A common strategy involves **specificity**, where precise details such as product names, discount percentages, or event dates are provided to enhance the sense of urgency. This specificity works in conjunction with the **time limitation** feature, which highlights deadlines or short time frames, urging victims to act swiftly in order to secure a perceived benefit. By framing the opportunity as fleeting or limited, attackers increase the psychological pressure on the victim to act impulsively.

Additionally, the **exclusivity** of the offer is emphasized, often suggesting that the victim has access to a unique or one-time opportunity, further motivating them to take immediate action. The use of phrases like "*last chance*" or "*only a few units available*" enhances the feeling of scarcity, reinforcing the urgency to act before the offer disappears. Similarly, references to potential **negative consequences** (such as penalties or loss of access) heighten the stakes and push victims to act quickly to avoid perceived harm.

Reflexive verbs (Figure no. 4) are frequently used in phishing e-mails that evoke a sense of urgency because they help create a personal connection between the sender and the recipient, thus amplifying the perception of immediate need. This strategy is motivated by the fact that **calls to action** that involve self-references can induce a state of anxiety and panic, causing victims to react impulsively, without critically analyzing the legitimacy of the message, which increases the effectiveness of cyberattacks.

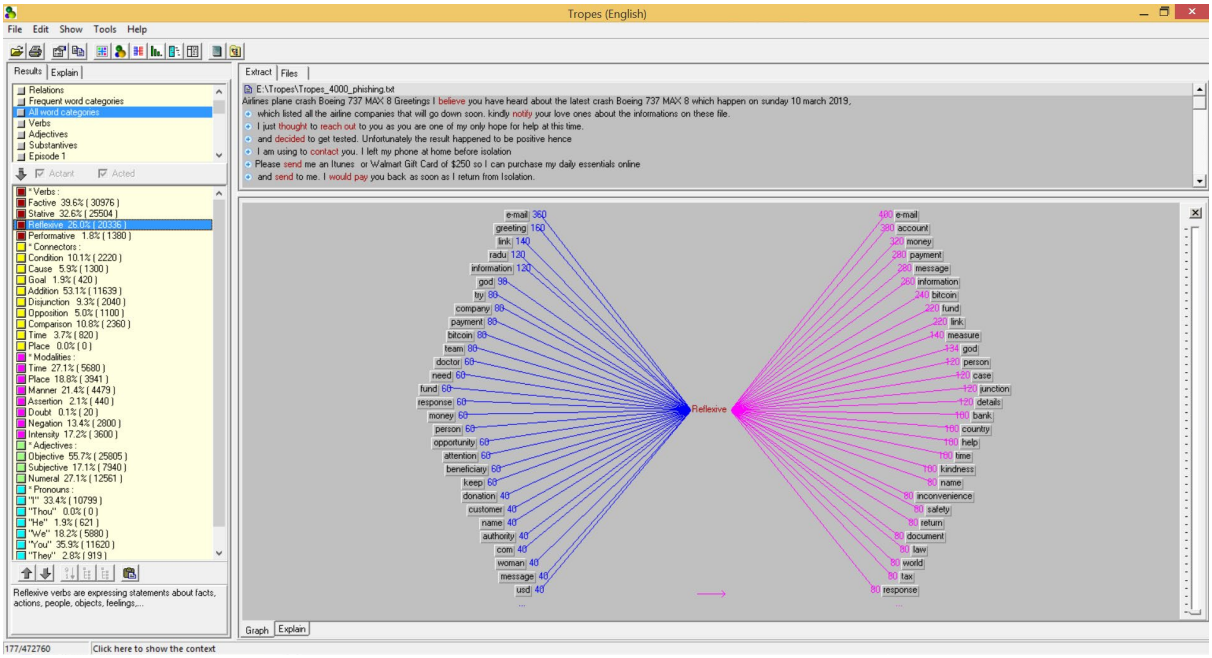

Figure no. 4: *Some reflexives from phishing e-mails identified by "Tropes"*
(Source: Authors' creation)

In phishing attacks that exploit the feeling of *sympathy*, attackers employ semantic constructs designed to foster a sense of trust, emotional connection, and closeness between themselves and the victim. The underlying strategy is to evoke feelings of **empathy** and **friendship**, encouraging the victim to respond without critically evaluating the information. The objective is to create a bond in which the victim feels emotionally compelled to act, often without a rational assessment of the situation:

– *"The trust I have in you has led me to send you this message. I hope you will not hesitate to give me your support"* (trust, support, hope);

– *"Please do not disappoint me. I urgently need your help with a personal matter"* (urgency, personal need, request).

Key elements in these attacks include the expression of **sincere support**, where attackers frame themselves as empathetic figures offering help or advice, seeking to elicit a response based on shared **human connection**. This is often coupled with the suggestion of a **mutual relationship**, wherein the attacker appeals to feelings of **trust** and **reciprocity**. By invoking prior positive interactions, such as "*I consider you a close friend*", attackers aim to deepen the emotional involvement, thereby increasing the likelihood of compliance. Additionally, the attacker may offer **personalized communication**, giving the impression of a familiar and intimate relationship, which serves to lower the victim's guard and provoke an emotional reaction.

In this context, the use of **empathy** or the expression of **gratitude** for previous assistance increases the sense of moral obligation, nudging the victim towards a perceived reciprocal action. Phrases such as *"you have always been there for me"* encourage the victim to act out of a sense of **obligation** or **loyalty**. Furthermore, the attackers frequently include an urgency element, asserting the need for immediate action, thus exploiting the emotional pressure to act quickly.

In *vanity* phishing attacks, attackers utilize semantic constructs designed to exploit the victim's desire for recognition, admiration, and elevated status. These messages aim to evoke feelings of

exclusivity, **pride**, and a sense of **superiority**, suggesting that the victim is distinguished or part of a select group. The language used emphasizes the **importance** and **uniqueness** of the victim, often framing them as deserving of special treatment or access to opportunities that set them apart from others. The goal is to trigger a response from the victim based on their perceived higher rank, often by offering rewards, recognition, or elite privileges:

– *"Be recognized for your outstanding achievements and receive a special award. Details inside"* (outstanding achievements, special award);

– *"Only the elite have access to this opportunity. We congratulate you on being part of this select category"* (elite, select category, congratulations).

The semantic features typically employed include references to **exclusivity**, such as invitations to private or restricted events, or the promise of **special treatment**, such as VIP status or recognition for achievements. The attacker may also emphasize the **limited nature** of the opportunity, suggesting that only a select few are worthy of receiving the offer. Phrases such as "*you are one of the lucky ones*" or "*you have been chosen*" are used to create the illusion that the victim is part of a privileged group, further strengthening the appeal to their vanity.

The **use of flattery** and **prestigious titles** is a common tactic in these attacks, with messages designed to make the victim feel as though they have achieved something exceptional or belong to an exclusive circle. This may include language that alludes to their **outstanding achievements** or positions them as an influential figure who is being **recognized** for their contributions. The victim is then encouraged to act based on the desire to maintain or elevate their perceived social standing.

Both the keywords and linguistic patterns identified in this study can be used to train a ML system designed to detect phishing e-mails. By implementing advanced semantic analysis, the algorithm will be able to classify suspicious messages based on the emotional and psychological exploitation used in the header. This methodology can significantly improve the effectiveness of security filters and automatic detection systems, thus helping to protect users against cyber threats.

5. Discussion

Phishing detection methods based on NLP have evolved significantly, employing various techniques such as ML models, DL architectures, and rule-based systems. The proposed approach, which utilizes the "Tropes" software for linguistic analysis, offers distinct advantages and limitations when compared to these more advanced NLP-based techniques. The comparison is evaluated across three key dimensions: efficiency, computational complexity, and availability.

The "Tropes" software specializes in linguistic analysis by identifying recurring semantic structures and categorizing textual elements based on predefined lexical databases. It is particularly effective in analyzing the psychological and rhetorical aspects of phishing e-mails, such as fear appeals, urgency, or authority-based manipulation. The rule-based nature of "Tropes" allows for quick processing of text data without requiring extensive training or labeled datasets. However, this method may be limited in adaptability to evolving phishing techniques, as it relies on predefined linguistic patterns.

Modern NLP techniques, such as those based on ML and DL, can analyze phishing e-mails with greater flexibility. These models can learn from large datasets and detect previously unseen phishing tactics by identifying latent linguistic features. While they typically achieve higher accuracy, their performance depends heavily on the quality and diversity of training data. DL models, in particular, can outperform rule-based methods

in recognizing sophisticated phishing attempts that deviate from traditional patterns.

While "Tropes" is efficient for predefined linguistic analysis, NLP-based methods are more adaptable and scalable, making them superior for detecting novel phishing strategies. However, NLP-based models require significant data preprocessing and feature engineering, which can slow down deployment in real-time scenarios.

"Tropes" operates as a lightweight linguistic analysis tool, requiring minimal computational resources. Since it primarily relies on rule-based categorization rather than statistical learning, it does not necessitate GPU acceleration or large-scale training datasets. This makes it suitable for environments with limited computational capacity, such as embedded security solutions or resource-constrained systems.

In contrast, NLP models – particularly DL approaches – require substantial computational resources. Training a model such as BERT or GPT-based classifiers demands high-performance hardware and significant storage for labeled phishing and legitimate e-mail datasets. Even traditional ML models, while less resource-intensive than deep learning, require extensive text preprocessing, feature extraction, and vectorization, which contribute to computational overhead.

The "Tropes"-based method is computationally efficient, making it more accessible for real-time phishing detection in low-resource settings. However, this comes at the cost of adaptability, as rule-based methods struggle with unseen phishing tactics. NLP-based models, while computationally expensive, offer superior detection capabilities but may not be feasible for every deployment scenario, especially in real-time filtering systems where processing speed is critical.

"Tropes" is a free-to-download linguistic analysis tool, which makes it an accessible option for researchers and cybersecurity professionals. However, despite its accessibility, the tool requires highly specialized knowledge to interpret the results effectively. The raw semantic interpretations provided by "Tropes" cannot be used directly but must be analyzed and contextualized by an expert in linguistics. Moreover, "Tropes" has notable functional limitations:

– It does not support direct comparative analysis of multiple texts, meaning users must manually open multiple instances of the application to perform comparisons;

– The semantic analysis of short texts is less relevant, which can be a drawback when analyzing phishing e-mails that often contain concise messages;

– Language support is limited to only five languages (English, French, Spanish, Portuguese, and Romanian), restricting its applicability for phishing e-mails in other languages.

Many NLP-based phishing detection methods are built on open-source frameworks such as TensorFlow, PyTorch, and Scikit-learn. These tools are widely accessible, allowing researchers and developers to create custom models suited to their specific needs. Unlike "Tropes", NLP models do not require expert interpretation of linguistic outputs, as machine learning algorithms automate feature extraction and classification. Additionally, NLP approaches:

– Allow for comparative analysis across large datasets, enabling automated detection of patterns across multiple e-mails;

– Are highly adaptable, supporting multiple languages if trained with multilingual corpora;

– Can be integrated into real-time phishing detection systems, making them more practical for cybersecurity applications.

While "Tropes" is freely available and easy to install, its usability is limited by the need for expert interpretation, inability to compare multiple texts within the software, and restricted language support. In contrast, NLP-based models, while requiring technical expertise to develop and deploy, offer greater flexibility, automation, and broader language coverage.

6. Conclusions

Despite the fact that the "Tropes" software has not received recent updates (the last version dates back to 2018), it remains a valuable tool for extracting semantic features from phishing e-mails, providing a complex interpretive framework that can complement and enhance methods based on artificial intelligence (AI), ML, and NLP.

One of the main advantages of "Tropes" lies in its ability to perform in-depth semantic analysis, identifying not only word frequency, but also relationships between concepts, communicated intentions, and persuasive strategies used in phishing messages. This level of interpretation can contribute to training AI and ML models, providing a set of relevant semantic features that can be used as input for NLP algorithms, thus improving the accuracy of phishing classification.

"Tropes" is also an accessible, easy-to-use tool that can operate independently of advanced computational resources, making it a viable option for exploratory phishing analysis before implementing more sophisticated AI solutions. By integrating the results provided by "Tropes" with modern NLP techniques, a hybrid system can be obtained that combines deep linguistic analysis with the efficiency of ML algorithms, thus increasing the ability to detect phishing attacks.

The results obtained underline the need for a multidisciplinary approach in combating phishing actions. In addition to technical security measures, it is essential to increase user awareness of the linguistic and psychological tactics used by attackers. Cyber education, information campaigns and the development of phishing message detection tools based on semantic analysis can help reduce the effectiveness of these attacks and protect users.

This work provides a solid basis for future studies, which could explore in depth the impact of socio-demographic factors on vulnerability to phishing attacks, as well as the evolution of linguistic manipulation techniques used by attackers. By continuously analyzing these strategies, we can more effectively anticipate and counter cyber threats, building a safer online environment for all users.

REFERENCES

Bagui, S., Nandi, D., Bagui, S., & White, R.J. (2019). Classifying Phishing Email Using Machine Learning and Deep Learning. *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. DOI: 10.1109/CyberSecPODS. 2019.8885143. Available at: https://monkey.org/~jose/phishing/.

L'Huillier, G., Hevia, A., Weber, R., & Ríos, S. (2010). Latent semantic analysis and keyword extraction for phishing classification. *2010 IEEE International Conference on Intelligence and Security Informatics*. DOI: 10.1109/ISI.2010.5484762.

Molette, P. (2009). *De l'APD à Tropes: comment un outil d'analyse de contenu peut évoluer en logiciel de classification sémantique généraliste*. Communication au colloque Psychologie et communication Tarbes. Available at: https://www.tropes.fr/PierreMolette-CommunicationColloquePsychoTarbesJuin2009.pdf, accessed on August 7, 2024.

Park, G., & Taylor, J.M. (2021). *Towards Text-based Phishing Detection*. arXiv.org. DOI:10.48550/arXiv.2111.01676.

Salloum, S.A., Gaber, T., Vadera, S, & Shaalan, K. (2022). A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques. *IEEE Access, Vol. 10*, 65703-65727. DOI: 10.1109/ACCESS.2022.3183083, Electronic ISSN: 2169-3536.

Tropes. (n.d.). Available at: https://www.tropes.fr/.

Zhang, X., Zeng, Y., Jin, X.-B., Yan, Z.-W., & Geng, G.-G. (2017). Boosting the phishing detection performance by semantic analysis. *2017 IEEE International Conference on Big Data (Big Data)*. DOI: 10.1109/BigData.2017.8258030.