How vulnerable are you? A Novel Computational Psycholinguistic Analysis for Phishing Influence Detection

Anik Chatterjee
St Thomas College of
Engineering and Technology
Kolkata, India
anikchatterjee63@gmail.com

Sagnik Basu
St Thomas College of
Engineering and Technology
Kolkata, India
sagnikbasu19@gmail.com

Abstract

This document contains our work and progress regarding phishing detection by searching for proper influential sentences. Currently, the world is becoming smart, as a result most of the transactions and posting offers happen online. So, human beings have become the most vulnerable to security breach or hacking through phishing attacks, or being persuaded through influential texts in social media sites. We have analyzed influential and non-influential sentences and populated our dataset with those. We have proposed a computational model for implementing Cialdini and we got state of the art accuracy with our model. Our approach is language independent and domain independent and it is applicable to any problem where persuation detection is important. Our dataset and proposed computational psycholinguistic approach will motivate researchers to work more in the area of persuasion detection.

1 Introduction

In some ways we humans are incredibly durable, and in others we are incredibly fragile. Most of the humans can be easily swayed by beautiful rewards. We are the most vulnerable to phishing attacks and such rackets. Some people take these opportunities to persuade people to click some bad links through some deceitful messages.

Susceptibility (Pierre O. Jacquet, 2018), persuasion (MakuochiNkwo and Orji, 2018; Kiemute Oyibo and JulitaVassileva, 2018; Ifeoma Adaji and JulitaVassileva, 2020; Christopher Hidey, 2018) and gullibility (Mercier, 2017), these three words are very much related to human behaviour. Humans are susceptible to treachery, they can be persuaded easily, and they are gullible too to believe anything in what others say.

Depending on a person's behaviour we can influence him/her using different types of methods. Robert Cialdini did research on all those methods and ways and published his famous principles. We created a classifier to detect types of influence by fine-tuning a pre-trained BERT model.

In this paper our major contributions are:

i. Our research on phishing detection was using computational psycholinguistic approach. Here we have modeled the Cialdini principles on influence analysis.

ii. We have prepared our dataset using influential texts, such as advertisements, Twitter posts etc.

iii. We experimented with pre-trained BERT models by adding extra layers and changing the learning rate.

The rest of the paper is organised as follows. Section 2 discusses about the related works and how those are different. Section 3 discusses about Cialdini principles and how we applied them in our work. Section 4 describes how we made our own dataset and related literature survey. Section 5 provides an insight into the pre-trained model and why we used it. Section 6 discusses about our experiment with different methods and tools to reach higher accuracy. Section 7 provides a detail about our result and section 8 concludes the paper.

2 Related Work

The closest research to our work is on sentiment analysis and persuasion detection based on Cialdini principles. Kiemute Oyibo and JulitaVassileva (2018) focused on how culture and gender influence the effectiveness of Cialdini's principles of persuasion. They investigated on how the culture,

Proceedings of the 18th International Conference on Natural Language Processing, pages 499–507
Silchar, India. December 16 - 19, 2021.

gender and age differences affect individual's susceptibility to Cialdini's persuasive strategies. But their work centred on the people of Nigeria. Sridhar Ramaswamy (2018) used unstructured data available for survey voice recording of customer interactions and chat transcripts and explored different technologies of Deep Learning (Goodfellow et al., 2016) and Natural Language Processing (NLP) that would help better analyze the contextual information to capture customer feedback. Christopher Hidey (2018) worked with detection of persuasion in online discussion or in some argument. Merton Lansley (2019) developed a method that detects social engineering attacks that are based on NLP and Artificial Neural Networks. Ifeoma Adaji and JulitaVassileva (2020) proposed the use of shoppers' online shopping motivation in tailoring six commonly used influence strategies: scarcity, authority, consensus, liking, reciprocity, and commitment and they identified how these influence strategies can be tailored or personalized to e-commerce shoppers based on the online customers' motivation when shopping. Shilpa P C (2021) used deep learning techniques to classify the sentiments of an expression into positive or negative emotions which were further classified into more atomic emotions. Vansh Gupta (2021) worked with persuasion detection but their work was based on biased or misleading information or propaganda classification.

Some researchers have also worked on sentiment analysis and persuasion detection based on Twitter data. OlhaKaminska and Hoste (2021) developed an approach for the SemEval-2018 emotion detection task, based on the Fuzzy Rough Nearest Neighbor (FRNN) classifier enhanced with Ordered Weighted Average (OWA) operators. Neha Jadav and Khamparia (2018) focused more on improvement of accuracy of sentiment system 1 to 5 star, 1 being the most negative.

So many works on persuasion detection have been done over the years. Everyone has focused on some particular domain, either customer feedbacks, online shopping sites, or some particular culture or area. Our goal was to identify phishing attacks through influential texts. Therefore we used persuasion detection and Cialdini principles and we tried to be more general in determining effects of these influences. So, we collected example sentences from as many diverse places as possible.

3 Our Technique

While searching for the ways by which people can be persuaded or phishing attacks can be detected we came across Cialdini's principles.[1] So we used mainly those principles in our classifier. Before going further let's first discuss about Cialdini principles.

3.1 Cialdini's Principles

Robert Cialdini published his book *"Influence: The Psychology of Persuasion"*[2] in 1984. In this book he explored some factors that affect the decisions that people make. Cialdini identified six core principles that affect this decision making process.

Reciprocity — People always tend to help those from whom they have got help before as a form of gratitude. So business companies make the advertisements in a way to provide their customers extra benefits, discounts, offers in order to prompt them to buy products from that company.

Scarcity — It is a fact that the less something there is, the more people will tend to want it. Many companies use this human behaviour to put some products in limited edition sale.

Authority — Individuals who are authoritative, credible, expert in their fields are more influential and persuasive than those who are not. People prefer to go for those company products that are promoted by authoritative figures.

Commitment and Consistency — People like them who are committed to their words, and they also like to be consistent with their identity. So many advertisements tend to make people believe something and make them do according to that. People also like to use the products which are committed to their usefulness.

Liking — People tend to follow those whom they love, that could be an authoritative person, a player, a singer. So some companies give such famous persons money to use their products and show to people.

Consensus — People love opinion of the majority. When they find something is used by most of the people they tend to use it too.

[1] https://worldofwork.io/2019/07/cialdinis-6-principles-of-persuasion/

[2] https://www.goodreads.com/book/show/28815.Influence

3.2 How we applied Cialdini theory

We used this Cialdini Persuasion theory in order to find the influence working behind a text, be it an advertisement or a text message. We made each category a class and thus we applied Cialdini's Principles as a multiclass Machine Learning (Mitchell, 1997) classification problem.

We chose Cialdini's principles to divide texts in multiple classes. We marked those classes as 1) Reciprocity, 2) Scarcity, 3) Authority, 4) Commitment, 5) Liking, 6) Consensus and we created a 7th class as not showing any influence, for normal sentences.

We collected email texts from different senders and went through different ads and categorized them according to the levels of persuasion.

Phishing attacks target vulnerabilities that exist in systems due to the human factor (Khonji et al., 2013). Many cyber attacks are spread via mechanisms that exploit weaknesses found in end-users, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. One of these techniques is persuasion analysis.

4 Making Dataset

We studied Cialdini's theory to understand how a person can be influenced in order to detect phishing attacks. We did not find any dataset regarding our research, so we had to make our own dataset and categorize the texts by ourselves. We used some pre-defined definitions in order to sort those sentences out. For identifying the six influence classes, we followed the following conventions —

- Give away or giving something without any charge on some occasion, such messages show reciprocity type of influence.
- Messages alerting customers regarding limited offer show scarcity type of influence.
- Messages or ads regarding sponsorship or doing partnerships show authority type of influence.
- Messages committing about well being or best performance of a product show commitment type of influence.
- Messages telling what one's favourite person uses or does, provoking him/her to use that product show liking type of influence.
- Messages showing survey results show consensus type of influence.

We collected as many influential texts as possible from advertisements from different companies and grouped them in those classes. We gathered about 100 texts from each class and made a dataset with 735 texts. We created a model using this dataset.[3]

Still the variety in our dataset was very small. So we collected more examples using twitter scraping of companies like – Amazon, Tesla, Microsoft, Flipkart, Tinder etc. From Amazon, Flipkart, we got more examples on scarcity and reciprocity. From Tesla, we got more examples on commitment types. Tinder gave us examples on liking. Big companies like these are also perfect for finding examples on authority and consensus. These sentences helped us understand how social sites can persuade people through influential advertisements and messages. After collecting these sentences on various domains we used our temporary model to make predictions. Then we rechecked, verified and corrected the predictions that were made above 95% and discarded others. Finally we appended those texts with our original dataset (please see table 1) and made its size 2379.

5 Used model for classification

5.1 Transformers vs RNNs

Transformers (Ashish Vaswani and IlliaPolosukhin, 2017) are semi-supervised machine learning models that were primarily used with text data and have also replaced Recurrent Neural Networks (RNNs) (Danilo P. Mandic, 2001) in Natural Language Processing (NLP) (Jurafsky and Martin, 2009) tasks. We chose Transformers for our problem because it beats RNN in time complexity.

Transformers use self-attention mechanism that allows the decoder to look back at the entire sentence and selectively extract the information it needs during decoding. This mechanism helps to know the context better. With RNN, one has to go word by word to access the cell of the last word. This becomes a major problem for GPUs,

[3] https://github.com/starboi2000/Phishing-detection-and-influence-analysis/blob/main/previous_data.xlsx

Sentence	Influence Class Number	Influence Class Name
@lifeisahandful You're most welcome! We're happy we can help brighten your day!	1	Reciprocity
@RachelLivesLife Thanks for the support! We are hiring, have a look.	1	Reciprocity
@JaggiPagal Apologies for the unpleasant experience with your order. Could you confirm if we've missed the estimated delivery date?	2	Scarcity
@FunSizeDel Time to bust out those happy moves, and dance All Night Long! Enjoy your order! #deliveringsmiles	2	Scarcity
@nhuebecker Alexa play The Fame by Lady Gaga	3	Authority
You guessed it - it's their next look! With the latest trends and top brands at Flipkart Fashion - India Ka Fashion Capital, there's no other way than to Wear the next!	3	Authority
You can now contribute to on-ground COVID relief services with #Check-OutGiving . Donate Rs. 10 to @GiveIndia when you check out with just a click of a button. #FlipkartCares #FlipkartForIndia.	4	Commitment
If you're not 100% in love after the first 30 nights, we'll pick it up, do all the packing, and give you a full refund. We do our best to donate returned mattresses and give them a new home.	4	Commitment
@StephTheGroupie You've got to be squidding! We're shrimply lobsessed with these slides. A pair of these would make anyone jelly(fish)!	5	Liking
@cutenfeisty– There's nothing quite like a good book journey! Tell us, what's your favorite genre of books to read on your Amazon Kindle device?	5	Liking
for the last 10 years we are the number 1 in this industry by our customer review	6	Consensus
57% of consumers will buy this or use a this service because it has at least a 4-star rating.	6	Consensus
Having Zelda's approval on the box just brightened up our Caturday! What does she enjoy doing when she's not lounging?	7	Normal
@pww3777 Someone sure looks comfurtable! What's this little cutie's name?	7	Normal

Table 1: Example Dataset

this sequentiality is an obstacle to the parallelization of the process. Whereas, transformer proposes to encode each position and to apply the mechanism of attention in order to connect two distant words, which can then be parallelized, accelerating learning.(Louis-Philippe Morency, 2018)

5.2 BERT vs Others

More than one architectures are being used in NLP tasks, such as ELMo, GPT, BERT.(Jacob Devlin, 2019)

ELMo follows a more traditional design and uses LSTM to compute vocabulary when it comes to art. BERT uses transformers in two approaches for language improvement. ELMo uses two layers each to include forward and backward passages to calculate the middle word vectors. This helps ELMo to achieve high efficiency compared to other traditional language models.(Ezen-Can, 2020)

Though transformer uses a decoder and an encoder, BERT only uses an encoder and it does bi-directional context search, whereas GPT does it in one direction. BERT can also be used for multi-masked sentences, and next sentence prediction, and bi-directional search really makes it more reliable. Moreover, BERT model reads at most 512 words in one iteration. GPT-3 has almost 175B parameters and T5 has 11B parameters, whereas

BERT has only 110M parameters in its base model and 340M parameters in its large model. Based on our subject we did not require so many parameters as GPT and T5 provide, that is why we preferred BERT over other models.

We picked BERT-base-uncased over cased as influence detection should not be sensitive to cases.

6 Experiments with different methods

We trained a wide range of different models for the task. As discussed in sections 3 and 4 we made our own dataset and used them to train the models. As we discussed in section 5, we used BERT model from transformers rather than RNN.

After making the train and validation datasets we applied different pre-trained models, fine-tuned them and used the best one to make our final model.

We fine tuned BERT-base-uncased with our Neural Network which is taking input from the fine tuned BERT layer and processing it in this extra 9 layers out of which first 7 layers are simple dense layers with the unit numbers of 1024, 512, 256, 128, 128, 64, 32, a dropout layer with 0.3 dropout rate and lastly an output dense layer with unit number of 7.

We fine tuned another BERT-base-uncased model with previous configurations but this time without the dropout layer. We wanted to check how it behaves after removing the dropout layer.

Then we also fine tuned a BERT-base-cased model with a total of 9 layers among which 7 layers are simple dense layers with unit numbers 1024, 512, 256, 128, 128, 64, 32, an output dense layer with unit number of 7 and one dropout layer with rate 0.3. We checked by removing the dropout layer also for this model.

Then we also fine tuned a Distilled version of BERT model or DistilBERT.

Our Deep Neural Network model used a vocabulary size of 10,000, a batch size of 32 and was trained over 10 epochs. The system consisted of two input layers, one main BERT layer, six dense layers with varying sizes decreasing from 1024 to 32, one dropout layer with regularization of 0.3 and one output layer.

We used Rectified Linear Unit (ReLU)[4] activation function for dense layers and Softmax function for the output layer. The main advantage of using ReLU over other activation functions is that it does not activate all the neurons at the same time. This means that the neurons will only be deactivated if the output of the linear transformation is less than 0.

We experimented with all these models using different learning rates, because not only the method, but how fast the model is learning, is also very crucial in gaining more accuracy. We started with 0.01 and decreased the rate each time until we got the maximum accuracy. Then we collected the learning rate and accuracy for each model. Among all these models, we got the best result in BERT-base-uncased without dropout layer model with learning rate of 0.0001 or 1e-4.[5]

7 Result and discussion

There are many datasets on whether a sentence is ham or spam[6][7] and datasets on detecting phishing sites[8](Justinas Rastenis, 2021; Patrick Lawson, 2020; Kiemute Oyibo and JulitaVassileva, 2018). But there is no dataset on influence analysis using Cialdini principles, so we had to make our dataset. Then we experimented with different Deep Neural Network models and found BERT-base-uncased to overwhelm others and be suited for our work.

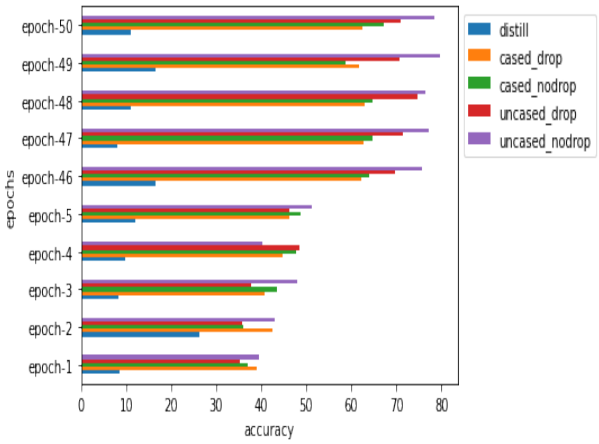

Figure 1: Accuracy Plot

Figure 1 shows epoch count versus accuracy for different models. We used the transformer models

[4] https://bit.ly/32YjPlx

[5] https://github.com/starboi2000/Phishing-detection-and-influence-analysis/blob/main/All_Codes_in_ipynb_to_understand_better/Cialdini_6_Principles.ipynb

[6] https://github.com/laxmimerit/All-CSV-ML-Data-Files-Download

[7] https://bit.ly/3lpxlFi

[8] https://bit.ly/32InPX6

DistillBERT, BERT-base-cased and uncased both of them with or without dropout. Among them we got the best result in BERT-base-uncased without dropout layer, we can clearly see in the graph above that the violet line is exceeding other lines in almost every epoch.

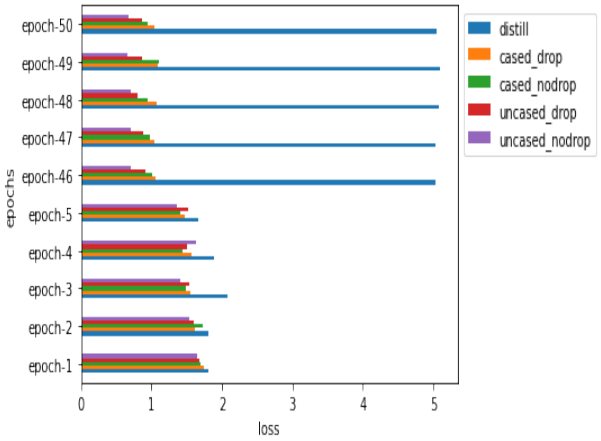

Figure 2: Loss Plot

Figure 2 shows epoch count versus loss for different models. As we got the best accuracy in accuracy graph for BERT-base-uncased without dropout, similarly we got the least loss in case of this model.

We used Bert-base-uncased model of Transformer to make our model with a learning rate of 0.0001 as it reached the highest accuracy. We achieved 97.46% accuracy with our small dataset. After appending it with more example texts, we got 93.76% from our model using the new dataset.[9]

We have also kept a sub-part[10] of the dataset, as our test data, and used that to evaluate our model. It turned out to be 87.5%.

Our model does not show which type of influence is being used, but rather it shows each type of influence along with their probabilities of being present in the given text.

Figure 3 shows the prediction of our proposed model by displaying the probabilities of each influence category in a given sentence.

To check this model is predicting well in the dataset, we used confusion matrix (See figure 4).

True Positive, False Negative, False Positive, True Negative for each class are shown in Table 3.

[9] https://github.com/starboi2000/Phishing-detection-and-influence-analysis/blob/main/main_data.xlsx

[10] https://bit.ly/3IcxPbs

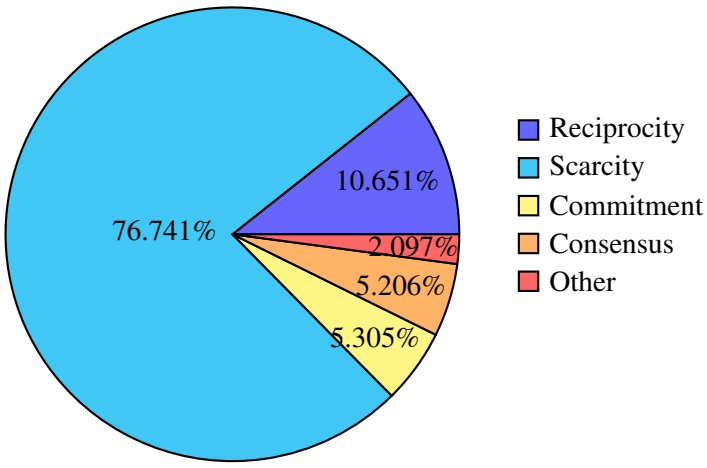

Figure 3: An example of the output

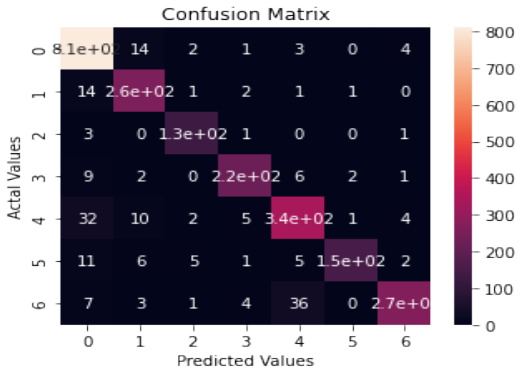

Figure 4: Confusion Matrix

Total number of true positive in 7 classes is 2176 out of 2379. We can see that we have the most information on Reciprocity type of influence and the least on Authority and Social Proof. As we have scraped business data, Reciprocity is the most dominant one there, and then comes Commitment. To make the understanding better we use F1-score which depends on both recall and precision.

In Table 2, we can check the F1-scores for different models on each class. We checked running all the models for 50 epochs. We can see that how we are getting the highest accuracy of 78% with the BERT-base-uncased model without a dropout layer.

8 Conclusion

Influence detection is a multi-level classification problem. Many works have been done on this topic and on persuasion detection, but they have worked on a particular domain, area, or caste. We focused more on finding the example texts not only from

	Reciprocity	Scarcity	Authority	Commitment	Liking	Consensus	Normal	Accuracy
Cased with dropout	0.81	0.66	0.42	0.44	0.52	0.25	0.6	0.63
Cased without dropout	0.83	0.65	0.39	0.6	0.6	0.3	0.67	0.67
Uncased with dropout	0.81	0.78	0.61	0.65	0.6	0.4	0.68	0.71
Uncased without dropout	0.87	0.8	0.7	0.77	0.7	0.65	0.76	0.78
Distil BERT	0.69	0.54	0.48	0.6	0.65	0.35	0.6	0.61

Table 2: F1-Score

	TP	FN	FP	TN
Class-0	810	24	76	1469
Class-1	258	19	35	2067
Class-2	127	5	11	2236
Class-3	224	20	14	2121
Class-4	338	54	51	1936
Class-5	153	30	4	2192
Class-6	266	51	12	2050

Table 3: TP, FN, FP and TN for each class

advertisements, but from normal messaging texts also.

We focused on detecting phishing and other social media attacks, because these are something to which people are the most vulnerable nowadays. We made our own dataset and we have not predicted only the type of influence; we have given all the probabilities for each type of influence. Even for a human, we cannot predict exactly what type of influence is working in a sentence. Sometimes, a sentence can be formed using more than one influence categories. Advertisements include multiple influences in one sentence, so that becomes very difficult for anyone to determine the most effective type of the sentence. So, we have shown the probabilities as a pie chart (please see figure 3) and also mentioned the type of influence that is most probably working.

Where from Here

i. At first we did not find any suitable dataset for our work, so we collected data from different advertisements and sentences from Twitter and we made our model. The final dataset that we have made is still not sufficient, so our model may be overfitted. We plan to increase the data more in the future using Bootstrap mechanism. Then by human intervention we will verify and rectify the predictions made by our model and train it with new data.

ii. We have fine tuned cased and uncased versions of pre-trained BERT model and we have also used DistilBERT. As our future work, we want to do more research using recent pre-trained models for better results.

iii. We have applied phishing detection using influence analysis in English language only. However, our proposed approach is domain and language independent. Therefore we are planning to apply our model for other Indian Languages starting from Bangla. We are also planning to see how it will work for fake news detection problem where influence detection is also important.

iv. Limited priorwork has been done on phishing detection using persuasion techniques. We did not have the opportunity to compare with those datasets. As a future work, we are planning to compare our dataset with different datasets and different methodologies.

References

Robert B. Cialdini 2004. The science of persuasion. In *Scientific American Mind 284, (2004), 76-84.*

Soumya Sahoo Ambik Mitra, Lambodar Jena. 2021. Emoji analysis using deep learning, advances in intelligent computing and communication (pp.689-698).

Niki Parmar Jakob Uszkoreit Llion Jones Aidan N. Gomez Lukasz Kaiser Ashish Vaswani, Noam Shazeer and IlliaPolosukhin. 2017. Attention is all you need. In *Conference on Neural Information Processing Systems*.

Kathleen McKeown Christopher Hidey. 2018. Persuasive influence detection: The role of argument sequencing. In *Proceedings of the AAAI Conference on Artificial Intelligence, 32(1)*.

Jonathon A. Chambers Danilo P. Mandic. 2001. In *Recurrent Neural Networks for Prediction: Learning Algorithms, Architectures and Stability*. [link].

Sabyasachi Mukhopadhyay Mrityunjoy Panday Deb Prakash Chatterjee, Anirban Mukherjee. 2021. A survey on sentiment analysis.emerging technologies in data mining and information security. In *Proceedings of IEMIS 2020, Volume 2 (pp.259-271)*.

Aysu Ezen-Can. 2020. A comparison of lstm and bert for small corpus. In *arXiv:2009.05451v1 [cs.CL]*.

Ian Goodfellow, Yoshua Bengio, and Aaron Courville. 2016. *Deep Learning*. MIT Press. http://www.deeplearningbook.org.

Kiemute Oyibo Ifeoma Adaji and JulitaVassileva. 2020. E-commerce shopping motivation and the influence of persuasive strategies. In *ORIGINAL RESEARCH, Frontiers in Artificial Intelligence*.

Kenton Lee Kristina Toutanova Jacob Devlin, Ming-Wei Chang. 2019. Bert: Pre-training of deep bidirectional transformers for language understanding. In *Annual Conference of the North American Chapter of the Association for Computational Linguistics*.

D. Jurafsky and J. Martin. 2009. In *Speech and language processing : an introduction to natural language processing, computational linguistics, and speech recognition*. [link].

Ivan Suzdalev Kornelija Tunaityte Justinas Janulevicius Antanas Cenys Justinas Rastenis, Simona Ramanauskaite. 2021. Multi-language spam/phishing classification by email body text: Toward automated security incident investigation.

Mahmoud Khonji, Youssef Iraqi, and Andrew Jones. 2013. Phishing detection: A literature survey. volume 15, pages 2091–2121.

Adaji Rita Orji Kiemute Oyibo, Ifeoma and JulitaVassileva. 2018. The susceptibility of africans to persuasive strategies: A case study of nigeria. In *Persuasive Technology International Workshop 2018*.

Kamil Halouzka Pavel Kozak Ladislav Burita, Petr Matoulek. 2021. Analysis of phishing emails.

Paul Pu Liang Soujanya Poria Prateek Vij Erik Cambria Louis-Philippe Morency, Amir Zadeh. 2018. Multi-attention recurrent network for human communication comprehension. In *Thirty-Second AAAI Conference on Artificial Intelligence*.

MakuochiNkwo and Rita Orji. 2018. Persuasive technology in african context: Deconstructing persuasive techniques in an african online marketplace. In *2nd African Computer Human Interaction Conference (AfriCHI'18)*.

Erik Cambria Md Shad Akhtar, Asif Ekbal. 2020. How intense are you? predicting intensities of emotions and sentiments using stacked ensemble. In *IEEE Computational Intelligence Magazine*.

Hugo Mercier. 2017. How gullible are we? a review of the evidence from psychology and social science.

Nikolaos Polatidis Merton Lansley and Stelios Kapetanakis. 2019. Seader: A social engineering attack detection method based on natural language processing and artificial neural networks. In *Computational Collective Intelligence*.

Stelios Kapetanakis Merton Lansley, Nikolaos Polatidis. 2019. A social engineering attack detection method based on natural language processing and artificial neural networks.

Tom Mitchell. 1997. In *Machine Learning*. [link].

Sagar Pande Neha Jadav and Aditya Khamparia. 2018. Twitter sentiment analysis using deep learning. In *IOP Conference Series: Materials Science and Engineering*.

Shervin Malmasi Mihaela Vela Liviu P Dinu Josef Van Genabith Octavia-Maria Sulea, Marcos Zampieri. 2017. Exploring the use of text classification in the legal domain. In *arXiv preprint arXiv:1710.09306*.

Chris Cornelis OlhaKaminska and Veronique Hoste. 2021. Fuzzy-rough nearest neighbour approaches for emotion detection in tweets. In *the IJCRS 2021 conference, organized jointly with IFSA-EUSFLAT 2021*.

Jennifer Carter Hamido Fujita Orestes Appel, Francisco Chiclana. 2021. Consensus in sentiment analysis. In *Fuzzy Logic (pp.35-49)*.

Deepak Upadhyay Oza Pranali P. 2020. Review on phishing sites detection techniques.international journal of engineering and technical research v9(04).

Aaron Crowson Christopher Mayhorn Patrick Lawson, Carl Pearson. 2020. Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy.

Andrea Desantis Yi-Fang Hsu Lionel Granjon Claire Sergent Florian Waszak Pierre O. Jacquet, Valentin Wyart. 2018. Human susceptibility to social influence and its neural correlates are related to perceived vulnerability to extrinsic morbidity risks.

Bennett Kleinberg Alexandra Lefevre Rada Mihalcea, Veronica Perez-Rosas. 2017. Automatic detection of fake news. In *arXiv:1708.07104v1 [cs.CL]*.

Katia Sycara Rahul Radhakrishnan Iyer. 2019. An unsupervised domain-independent framework for automated detection of persuasion tactics in text.

Susmi Jacob Vinod P Shilpa P C, Rissa Shereen. 2021. Sentiment analysis using deep learning. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*.

Akira Yamada Avumu Kubota Shoma Tanaka, Takashi Matsunaka. 2021. Phishing site detection using similarity of website structure. In *IEEE Conference on Dependable and Secure Computing (DSC)*.

Manish Kumar Shubham Khera. 2020. The comparative analysis with bert and elmomethods for movie reviews prediction using nlp.

Sriparna Saha Pushpak Bhattacharyya Shweta Yadav, Asif Ekbal. 2018. Medical sentiment analysis using social media: towards building a patient assisted system. In *Proceedings of the Eleventh International Conference on Language Resources and Evaluation (LREC 2018)*.

Natalie DeClerck Sridhar Ramaswamy. 2018. Customer perception analysis using deep learning and nlp complex adaptive systems conference with theme: Cyber physical systems and deep learning.

Pushpak Bhattacharyya Subhabrata Mukherjee. 2012. Feature specific sentiment analysis for product reviews. In *International Conference on Intelligent Text Processing and Computational Linguistics*.

Raksha Sharma Vansh Gupta. 2021. Roberta model with data augmentation for persuasion techniques detection.