Advances in Military Technology
Vol. 19, No. 2, 2024, pp. 225-241
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.01873

Phishing – Still Topical

L. Buřita*, K. Halouzka and P. Kozak

Department of Informatics and Cyber Operations,
University of Defence, Brno, Czech Republic

The manuscript was received on 6 December 2023 and was accepted after revision for publication as a case study on 8 October 2024.

Abstract:

The article summarizes the results of research into phishing threats and attacks over a multi-year period. Obtained phishing emails are subject to statistical, frequency, and content analysis; messages are classified according to the content into five segments: Business, Fund, Charity, Transfer, and Others. An experiment of communicating with phishing attackers is described; necessary security measures are set for this. Protection against phishing attacks is solved by filtering incoming mail on the Microsoft Outlook client while applying rules with keywords obtained from individual segments. In a broader context, the cyber security of email communication is explained, and commercial tools for defense against phishing attacks are described. The usability of research results is also assumed in the education of university students and the training of employees of companies and organizations.

Keywords:

phishing, analysis, classification, communication with phishers, defense, education

1 Introduction

The article deals with phishing threats and attacks sent by email messages and follows up on the research carried out over the past three years. First, the basic terms will be explained.

Phishing is a procedure that has been used for decades, in which the attackers send the recipients a fraudulent email and try to lure them into handing over information, downloading a suspicious attachment, or clicking on a fraudulent link based on an offer to obtain some benefit from potential cooperation.

The most successful phishing emails contain lures that act as psychological triggers so that the users react quickly to act out of a sense of moral obligation, greed or ignorance. Phishing is the first step in almost all cyber-attacks. The most dangerous is spear phishing, an individual and targeted attack on important victims, which yields sufficient profit, using carefully prepared communication.

* *Corresponding author: Department of Informatics and Cyber Operations; Faculty of Military Technology, University of Defence, Brno, Kounicova 156/65, CZ-662 10 Brno, Czech Republic. Phone: +420 973 44 21 72, E-mail: ladislav.burita@unob.cz*

Phishing does not apply only to emails but the same risk can be expected in other formats of instant messaging, and attacks using SMS messages (smishing); all as part of so-called social engineering. It is a method to gain access to systems and data using human psychology, instead of the technical tools of hackers.

The article is organized as follows: the Introduction is followed by a Literature Review, Methodology, and used Tools; further Analysis of Phishing Emails, Analysis of Keywords in Phishing Messages, Communication with a Phisher, Security Policy, Education, and Defense Against Phishing Attacks then the Conclusion, and References.

2 Literature Review

Email is an indispensable form of communication. Research has shown that people often fall victim to phishing attacks. This occurs in controlled experimental conditions as well as in real-world environments, although phishing awareness training is ongoing. The article [1] deals with the effect of interruption of concentration at work on the ability to correctly assess the possibility of a phishing attack. Disruption is a widespread phenomenon and has been shown to negatively affect performance in many activities. This study aims to determine the effect of interruptions in the processing of experimental tasks on the classification of phishing emails. Participants performed a task in which they categorized emails as phishing or legitimate. During the experiment, they were occasionally interrupted by either a secondary task to complete or an empty pop-up window. The results of both experiments indicated a higher accuracy of phishing classification when the action was interrupted. The findings suggest that interruptions during a phishing classification task can increase the likelihood of correctly identifying a phishing attack.

Phishing attacks have evolved considerably in recent years. This development has fueled a growing interest in research into an anti-phishing strategy known as an identity-based detection technique [2]. Identity-based detection techniques can achieve significant success in the rapidly changing phishing landscape. This is due to the brand identity inherent in most legitimate websites. Existing identity-based techniques suffer from a higher false-positive rate due to the complexity and difficulty of establishing a website's brand identity. To overcome the existing shortcomings, it is necessary to create a hybrid detection technique that uses the visual and textual identity of web pages. It has been empirically demonstrated on benchmark datasets that such a visual and textual identity detection procedure significantly improves phishing detection performance with an overall accuracy of 98.6 %. The achieved results, compared to the existing technique, showed a reduction of up to 3.4 % of misidentified input data. They confirmed a reduction in the misclassification of legitimate websites without sacrificing phishing detection performance.

Research [3] presents an integrated information processing model of phishing susceptibility based on previous research on information processing and interpersonal deception. It refines the model using a sample of intended victims of a real phishing attack. Overall, this model explains almost 50 % of the variation in individual susceptibility to phishing. The results suggest that most phishing emails are processed peripherally, with individuals making decisions based on simple cues embedded in the email. Urgent stimuli in the email stimulated increased information processing, thereby suppressing abilities that could potentially help detect fraud. Additionally, the findings suggest that habitual patterns of media use combined with high levels of email load have a strong influence on the likelihood that individuals will succumb to phishing. The sample of people used in the study was not representative of the general public, as only students were involved in research. They tend to engage more in online activities and conduct more online business transactions than the average consumer. Therefore, there are several limiting factors of the study. It tested only a limited number of phishing emails which were similar in the types of information they asked for and the level of threat they posed. Differences in the quality of phishing emails can increase individual susceptibility to phishing. Due to the lack of a control group, it is difficult to know whether the effects found in the study reflect just processing phishing emails or a reflection of general email usage behavior. Nevertheless, event taking into account these limitations, the research contributes to the understanding of phishing fraud. In fact, this study was the first to integrate different lines of research and test a variance-based model of phishing susceptibility.

The study [4] evaluates whether improved browser security indicators and increased awareness of phishing have led to improved user experience. Participants were shown a series of websites and asked to identify phishing websites. Eye tracking has been used to obtain data on which visual cues attract users' attention when determining the legitimacy of a website. Only 53 % of phishing sites were successfully detected by users. Time spent looking at browser elements correlates with an increased ability to detect phishing. The general technical proficiency of users does not correlate with improved detection scores. The effectiveness of browser design tweaks to help users identify fraudulent websites was evaluated. It examined human behavior and what the user looked at and for how long, using a device that measures eye movements. This was the first study to use eye-tracking data to identify security indicators that attracted users' attention to determine the legitimacy of websites. Participants' interactions with each web page were recorded and using eye-tracking data was captured, along with the time required for judgment.

Phishing attacks on websites continue to pose significant security challenges for both individuals and businesses, including identity theft, malware, and viruses. Although the performance of anti-phishing tools has improved significantly, it is unclear how effective these tools are at protecting users. The study [5], an experiment involving more than 400 participants, was used to evaluate the impact of the accuracy of anti-phishing tools on users ability to avoid phishing threats. Each of the participants was given a high accuracy (90 %) or low accuracy (60 %) tool and asked to make different decisions about several legitimate and phishing websites. The results of the experiment revealed that participants using a highly accurate anti-phishing tool significantly outperformed those using a less accurate tool in their ability to distinguish legitimate websites, avoid visiting phishing websites, and avoid transactions with phishing websites. However, even users of the highly accurate tool often ignored the correct recommendations, resulting in a success detection rate of approximately 15 % lower than that of the anti-phishing tool used. As a result, on average, participants visited 74 % to 83 % of phishing sites and were willing to trade with up to 25 % of phishing sites.

The goal of the papers [6] and [7] is to analyze the capabilities of cluster users of a selected network based on their browsing behavior. The source of the information is the web access log file, which contains all the important information. The paper presents the idea of processing information from the web access log file. The presented methodology can also be used in the field of cyber defense. The availability of commercial communication systems that are available in the market can create a high probability of exploiting backdoors and other weaknesses by attackers. It is essential to know what pages a particular user views. User behavior can be identified by analyzing the websites visited. The source of information is the knowledge from navigation on the user's website. The most frequently used methods are ontological profiling or conceptual clustering. Another approach to this task is a generalization-based clustering method which first generalizes the relationships and then uses a hierarchical algorithm to identify clusters in the source data. The information collected covers the types of pages visited by the user over time and how the user moves from one page to another.

Efficient generation of hash functions is very important to achieve security in networks. Recurrent neural networks as a possible approach could be used to generate hash functions. The performance of the recurrent neural network (RNN) has been verified by using a software implementation of RNN for a given network configuration. The principles of recurrent neural networks and their practical applications for hashing are presented in [8]. Secure communication is an important part of the Internet. Commercial communication systems are easy to use but can be exploited by an adversary. There are many examples of attacks on communication infrastructure. The structural complexity of artificial neural networks creates major obstacles to their use in real applications. The structural complexity of ANNs goes with the structure of the network.

3 Methodology and Used Tools

The data preprocessing includes the creation of a text file with a chronological record of phishing emails and their gradual storage as individual files with a unique number.

At the same time, emails are statistically and content evaluated (email source, request to send personal data, pressure for a quick response, stated amount of money); they are further divided into groups following the results of previous research (Business, Fund, Transfer, Charity, Others). With SW Tovek, so-called entities (names of persons, email addresses, websites, cities, and countries) are obtained from email messages. The tool for analyzing phishing emails is SW Tovek [9] with components:

- Index Manager – email indexing,
- Tovek Agent – text search,
- Info Rating – contextual analysis,
- Harvester – content analysis.

Word analysis of email messages was processed using Harvester, which, in addition to the list of words, also provides their score (the number of emails where the word occurs).

Security measures have been taken to communicate with phishing attackers:

- communicate via fake identity,
- use networks outside of the university for communication,
- do not provide personal information, download suspicious attachments, or click on the sent web pages.

4 Analysis of the Phishing Emails

The chapter deals with the analysis and classification of phishing emails. Emails from 2021, 2022, and 2023, which were obtained from the university email box of the author of the article, each year for one month, are processed. The following chapter deals with the word analysis of phishing emails to select keywords for filtering them.

4.1 Statistical Analysis

The statistical analysis starts with a basic survey of phishing emails according to the general parameters listed in Tab. 1. The personal email parameter clarifies that a sender is a private person; if the sender is a business company or any other organization, it is a corporate email. The parameter “contains the name of the sender clarifies that the given email contains the personal or corporate names of the senders.

Personal information is mostly the goal of phishing; if personal information is required in the mail, the parameter “required basic pers-info” is applied (it includes name, phone, and address). The parameter “required detailed pers-info” explains that even more information is required (occupation, sex, nationality, date of birth, etc.). The parameter “required pers-info fill in the form requires to fill personal information into the attached form, and “required pers-identification” aims to gain personal documents (identification card, passport, letter of recommendation).

The following parameter “required account number means the request to send the bank account number and the next parameter “requires a quick response is characterized by the usual request by the phisher for an immediate response. The last two parameters of Tab. 1 are the sum of money or volume of gold promised in phishing emails. The statistical analysis continues with an overview of the number of attacks (frequency analysis) in the individual weeks of the monthly measurement, see Fig. 1.

Tab. 1 General parameters of phishing emails

Parameter / Message		**2021**		**2022**		**2023**	
2021 (88), 2022 (78), 2023 (51)		**Sum**	**%**	**Sum**	**%**	**Sum**	**%**
1	personal mail	60	68	45	58	22	43
2	corporate mail	28	32	33	42	29	57
3	contains the sender’s name	83	94	70	90	46	90
4	required basic pers-info	7	8	5	6	2	4
5	required detailed pers-info	14	16	19	24	11	22
6	required pers-info fill in form	3	3	3	4	0	0
7	required pers-identification	7	8	10	13	5	10
8	required account number	3	3	1	1	1	2
9	required a quick response	68	77	30	38	11	22
10	money [mil. USD]	943	–	485	–	153	–
11	gold [kg]	337	–	0	–	3.4	–

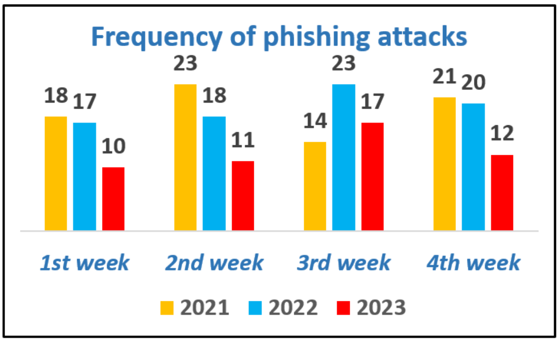


Fig. 1 Frequency analysis of the phishing attacks

The overview shows a relatively stable situation, even though the last year of the measurement meant a slight decrease.

4.2 Classification of Phishing Emails

The content analysis was carried out from several points of view and also the Tovek tool was used. The emails are classified according to the content of the email message into five segments: Business, Fund, Charity, Transfer, and Others. Each of the segments is described in even more detail (see Tab. 2); segments are briefly characterized and an example of the word connection with the most cited keyword is depicted.

Tab. 2 Segments of phishing emails in detail

Message content		2021		2022		2023	
		Sum	%	Sum	%	Sum	%
I	**BUSINESS**	**28**	**32**	**21**	**27**	**12**	**24**
1	Project, contract or investment	21	24	12	15	5	10
2	Offer trading, goods and services	2	2	8	10	5	10
3	Job, immigration offer	5	6	1	1	2	4
4	Payment for services	0	0	0	0	0	0
II	**FUND**	**14**	**16**	**29**	**37**	**17**	**33**
1	Gift, prize, award	3	3	6	8	4	8
2	Fund of bank, compensation, corona	4	5	17	22	7	14
3	Contractor of the fund; to share fund	5	6	1	1	1	2
4	Inheritance	2	2	5	6	5	10
III	**CHARITY**	**19**	**22**	**5**	**6**	**3**	**6**
1	Charity due to a fatal illness or God promise	16	18	3	4	0	0
2	Charity project, request for support	3	3	2	2	3	6
IV	**TRANSFER**	**23**	**26**	**14**	**18**	**8**	**16**
1	Money from bank to receiver account	21	24	11	14	7	14
2	The pick-up shipment, boxes with money	2	2	3	4	1	2
V	**OTHER**	**4**	5	**9**	**12**	**11**	**22**
1	Loan offer	1	1	0	0	0	0
2	Incoming mail blocked, undelivered shipment	0	0	1	1	1	1
3	Reminder of the previous message	0	0	2	3	2	2
4	Offer friendship, community	0	0	0	0	1	1
5	Unblocking/actualize a bank account	0	0	0	0	2	2
6	Unspecified message, call to communicate	2	2	6	8	5	5
7	Conference invitation	1	1	0	0	0	0

Business Segment

The segment includes phishing emails, in which cooperation on a contract, project, investment action, or other realization of a business opportunity is offered. The partner offers a product or service, employment with a high salary with lucrative benefits.

Keywords: *assistance, **business**, capital, company, consultant, development, employment, industry, insurance, investment, job, loan, manufacturer, position, product, resource, sector.*

The most cited keyword *business* of the Business segment and keyword *cancer* of the Charity segment with their word connections is seen in Fig. 2.

Fund Segment

The segment includes phishing emails that promise money or other assets from the funds (scams or fraud compensation, COVID-19, etc.). The content of the phishing emails in the segment may be a gift or inheritance.

Keywords: *award, bank, benefit, board,* ***fund****, identification, inheritance, lottery, notification, payment, prize, receipt, recipient, verification, winning.*

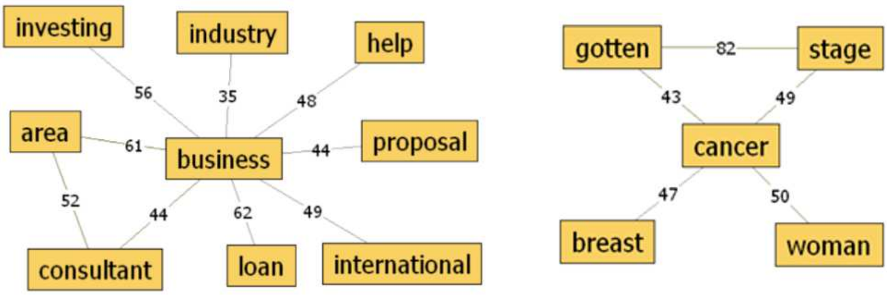


Fig. 2 Word connection with keyword business and cancer

Charity Segment

The segment includes emails that contain a story of an old woman, a widow whose large fortune (millions USD) was left by her deceased husband, which she wants to donate to charity. She complains of a fatal illness and is referring to God and Christian love. The next reason for the mail of the charity segment is an offer of the project.

Keywords: *breast,* ***cancer****, death, disease, doctor, god, fund, health, help, hospital, charity, illness, orphanage, suffering, trust.*

Transfer Segment

The segment includes emails in which the phisher would like to cooperate in the money or any other assets transfer. The commission for transfer is between 30 to 60 %. The potential initiator is a bank clerk who discovered a money account and claims that it is a completely risk-free operation.

Keywords: *accountant, agreement, airport,* ***bank****, box, credit, deposit, embassy, lawyer, package, transfer.*

Segment Others

The segment includes emails of marginal significance: unspecific offers, repeatedly notified contacts, undelivered packages, loan offers, and conference invitations.

Keywords: *account,* ***benefit****, business, conference, contact, greeting, mail, message, need, package, response.*

4.3 Content Analysis

The result of the search in SW Tovek is not only a list of documents relevant to the question asked but also a list of so-called entities. To illustrate the content analysis, we will display an overview of countries and cities that were mentioned in phishing emails. Most cities that appeared in phishing emails (11) were from the United States. Only one to three cities appeared from the other states, quite a varied overview, see Tab. 3.

Tab. 3 Overview of cities in phishing emails

	Country of the city	Entity city		Country of the city	Entity city
1	Australia	Gold Coast, Sydney	15	New Zealand	Christchurch
2	Benin	Cotonou	16	Nigeria	Abuja, Lagos
3	Brazil	Santos	17	Oman	Muscat
4	Canada	Hamilton, Surrey	18	Philippines	Floridablanca, Manila
5	Cote d'Ivoire	Abidjan	19	Spain	Salamanca
6	France	Paris	20	South Africa	Johannesburg
7	Ghana	Accra	21	South Korea	Seoul
8	China	Hong Kong	22	Switzerland	Genève, Zürich
9	India	Durg, New Delhi	23	Thailand	Bangkok
10	Indonesia	Jakarta	24	Togo	Lomé
11	Jordan	Amman	25	Turkey	Istanbul
12	Malaysia	Alor Setar	26	United Arab Emirates	Abu Dhabi, Dubai
13	Mexico	Ciudad del Carmen	27	United Kingdom	Bristol, London, Stanley
14	Morroco	Salé	28	United States	Atlanta, Corona, Fargo…

5 Analysis of Keywords in Phishing Messages

The frequency analysis of words from phishing emails is processed on the data analyzed in Chapter 4 from the segment point of view, using the SW Tovek. The goal is an analysis that will be useful for selecting keywords for filtration emails in the mail client to block them.

5.1. Keywords for Classification Phishing Emails

The analysis is focused on emails from the Business, Fund, Transfer, and Charity segments, the Others segment has been omitted. The Harvester module from the Tovek Tools SW package was applied for word selection. The statistics of word selection and processing are shown in Tab. 4. The weight of words from the analyzed emails, given by the number of found in the emails, further characterizes each word.

Tab. 4 Statistics of word processing

	Segment	Email	Words-Orig	Words-1.ph	Words-2.ph
1	Business	66	266	73	25
2	Fund	64	302	65	17
3	Transfer	45	224	60	8
4	Charity	27	120	36	12

Explanations to Tab. 4:

- Email = number of emails in analysis,
- Words-Orig = some words from the emails,
- Words-1.ph = number of words after the 1st phase of the processing,
- Words-2.ph = number of words after the 2nd phase of the processing.

In the 1st phase of word reduction, words that have no meaning for the search were omitted (STOP words). Subsequently, the resulting list of words was arranged according to the number of their occurrences in emails.

In the 2nd phase, only the original words in each segment that did not occur in another segment remained. Words that require sending personal data and names of family members in a phishing message have been deleted, such as *name, address, occupation, phone, country, nationality, and passport; family, father, child, daughter, husband, and widow*.

Typical words from more segments included the topic of business cooperation proposals: *business, contact, contract, compensation, confirmation, cooperation, delivery, charity, investment, joint, opportunity, partner, project, proposal, relation, security, service, support, transaction, transfer, technology, venture; from the field of finance and to describe the organization: airport, bank, claim, client, customer, dollar, donation, finance, fund, gold, government, law, money, payment, price.*

Resulting keywords from the segment (selection):

Business – *assistance, capital, development, job, position, product, resource, sector.*
Fund – *award, board, inheritance, notification, receipt, recipient, verification, winning.*
Transfer – *accountant, agreement, banker, box, credit, deposit, embassy, lawyer.*
Charity – *cancer, death, doctor, help, hospital, illness, orphanage, suffering.*

5.2. Keywords for Filtration of Phishing Emails

To obtain keywords for filtering phishing emails to increase the security of electronic communication, you need to proceed in the opposite way as in subsection 5.1.

On the contrary, the same words are selected in all segments to achieve effective capture of fraudulent messages. For the selection of words, the first rule was established that they must occur in at least three segments out of the four analyzed. The result is a set of 27 words: *account, address, bank, business, company, compensation, contract, country, dollar, family, finance, fund, God, government, money, name, officer, payment, personal, phone, project, proposal, security, service, telephone, transaction, transfer*. The filtering of phishing emails was gradually verified and corrected, based on the established rules in the MS Outlook client, see Tab. 5.

Tab. 5 Phishing evaluation

	1st phase	[%]	2nd phase	[%]	3rd phase	[%]
Phishing	62	100	40	100	33	100
False-positive	29	47	9	22	9	27
False-negative	1	2	3	8	6	18

The results at the first check were not acceptable, with almost a 50 % error rate. The rules were corrected primarily with words that should prevent false positives, especially as a result of sending messages about company events and conferences. Due to their influence, the error rate of filtering phishing emails decreased to 30 %, but the next phase worsened the results again. It is a permanent iterative and strictly individual process of tuning such filtering. You need to arm yourself with patience to achieve the optimal result.

5.3. Summary of Phishing Emails Analysis and Defense

The goal of analyzing phishing attacks is primarily to get to know them thoroughly and to learn what to expect from a phishing attacker. The results of the analysis will be used mainly in teaching and individual defense. For example, by filtering emails on MS Outlook, the email client uses the keywords of the phishing communication.

Such a way of defense is independent of the organization's cyber defenses and gives the individual a chance to defend themselves. Of course, it is not comparable to the organization's sophisticated cyber defense technology, but it is an option for individual defense, without intervention in the IT infrastructure, moreover, it is a strictly individual solution.

6 Communication with a Phisher

With the emergence of the internet as a widespread communication medium, fraud has also hit the digital environment. One of the most common forms of internet scams is phishing, where an attacker uses fake websites, tempting offers, and persuasion to try to lure sensitive data from the victim. There is also the inducement to engage in various forms of non-standard and sometimes anti-social behavior, or even some form of coercion or manipulation. Internet fraudsters try to gain access to bank accounts, personal information, or passwords.

6.1. Phishing in Communication

Phishing communications primarily take two forms - fake websites personal communications, and email correspondence. In the case of websites, the scams take the form of a trusted organization, such as a bank or other established organization. The victim is asked to enter a password; credit card or bank account details are requested.

The communication between a phishing attacker and their victim is characterized by several features that are indicative of attempted fraudulent behavior. A request to send sensitive data will certainly appear at an appropriate stage of the communication. Such requests are a clear example of phishing. Subsequently, there are two options for communication.

In the first option, the victim is exposed to a rapid succession of communications that cause stress from the incoming information. This creates a situation requiring an accelerated decision-making process. The victim becomes more focused on the possible loss of a lucrative offer or the possibility of losing out on a financial benefit, and their judgment and alertness are significantly impaired.

In the second option, longer communication delays can be used. This seemingly reduces the feeling of aggression and the victim, after a certain but generally short time, begins to perceive the attacker as a subject for a long time, and again the vigilance is reduced. The attacker becomes an accepted communication partner.

The next step is a gradual familiarization with the demands of the attacker. In this case, the victim's vigilance is blurred by the gradual communication of the attacker's demands. Such a situation leads to a reduction in susceptibility to potential danger. To a certain extent, the communication may rely on the unsubstantiated belief of the person addressed that such an attack cannot be carried out because it is easily recognizable.

6.2. Content of the Phishing Communication

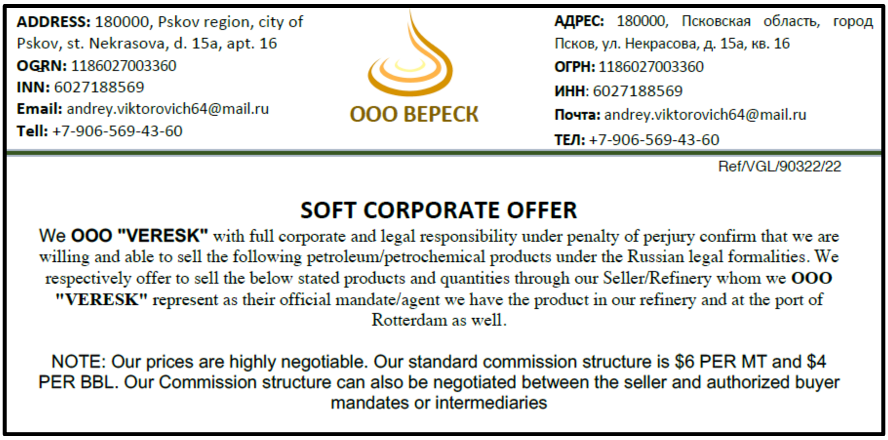
The victim must be captivated. Emails are often based on a very appealing way of addressing the victim. Often it is information about a large lottery win, the random drawing of an email address as the winner of a large sum of money donated by an eccentric philanthropist, or an off-the-cuff request for help from a victim in need. In the case of a prize, the victim is required to disclose sensitive personal information or pay a handling fee in advance. The payment of the prize may be conditional on other payment terms, such as demonstrating social conscience by immediately sending the amount of money to a charitable fund. This required amount of money is insignificant compared to the financial advantage offered.

Often there is a request for assistance in extracting a substantial sum of money deposited in an account whose rightful owner has died or is an account for which the owner has not been traced for a long time. The legality of the action is defended by different laws. The attacker assures that such actions are perfectly legal in the country where the alleged victim lives. Attackers are good at working with human emotions and target their offers towards high returns and easy financial security in the future or focus on compassion for the person in need. This is why there are open solicitations for financial contributions to charities.

6.3. Communication with a Phisher as an Experiment

The goal of the experiment including 100 phishing emails was to find out how communication with phishing attackers takes place. From this number of emails, only 68 were answered and at the same time, the most answers in communication (4, 5, and 6 times) were only once. The best source of emails for a phisher to answer was the non-specific content of the first email, it is possible to communicate with phishers without risk, provided that proper security measures (see Chapter 3).

Some interesting information was obtained, but the decision on whether a phisher is a person or a robot could not be confirmed with certainty. In terms of response speed, almost 20 % of emails with answers were obtained on the same day. During the phishing communication, the phisher tried more and more to argue that this was a fair discussion, not a scam. He adds attachments with personal data (see Fig. 4) or fictitious business documentation (see Fig. 3).



ADDRESS: 180000, Pskov region, city of Pskov, st. Nekrasova, d. 15a, apt. 16
OGRN: 1186027003360
INN: 6027188569
Email: andrey.viktorovich64@mail.ru
Tell: +7-906-569-43-60

ООО ВЕРЕСК

АДРЕС: 180000, Псковская область, город Псков, ул. Некрасова, д. 15а, кв. 16
ОГРН: 1186027003360
ИНН: 6027188569
Почта: andrey.viktorovich64@mail.ru
ТЕЛ: +7-906-569-43-60

Ref/VGL/90322/22

SOFT CORPORATE OFFER

We **OOO "VERESK"** with full corporate and legal responsibility under penalty of perjury confirm that we are willing and able to sell the following petroleum/petrochemical products under the Russian legal formalities. We respectively offer to sell the below stated products and quantities through our Seller/Refinery whom we **OOO "VERESK"** represent as their official mandate/agent we have the product in our refinery and at the port of Rotterdam as well.

NOTE: Our prices are highly negotiable. Our standard commission structure is $6 PER MT and $4 PER BBL. Our Commission structure can also be negotiated between the seller and authorized buyer mandates or intermediaries

Fig. 3 The business documentation

As an example of the communication and its progress, we are presenting the email exchange from the Fund segment. The initialization phishing email from Mr. Stephen Norris, of NORRIS & Associate in MADRID-SPAIN, a solicitor at law, was short. The attacker offered the fund cooperation, but the first suspicious fact was that the given email address was different from the sender's address. Remarque: Norris & Associates, Inc. is a manufacturer's representative serving the New England electronics marketplace.

After our positive response, an email was sent with information about the lucrative offer. The attacker was the personal attorney for the deceased Mr. Philip Malik (identical surname with our fake identity) from the United States, who is looking for his offspring for the settlement of the estate. It should be the last attempt before the inheritance is confiscated. Another suspicious circumstance of communication is the name of the deceased, which corresponds to our false identity.

The story of the deceased ends in the tsunami of 26th December in Indonesia in 2004 alongside his wife and only son while they were on vacation. Since then, all inquiries of the attorney to locate any of his client's extended relatives have been unsuccessful. Before the catastrophe that claimed his life, he had a contract with Repsol and British Petroleum which filed for a claim on his behalf, and the payment has been released and deposited.

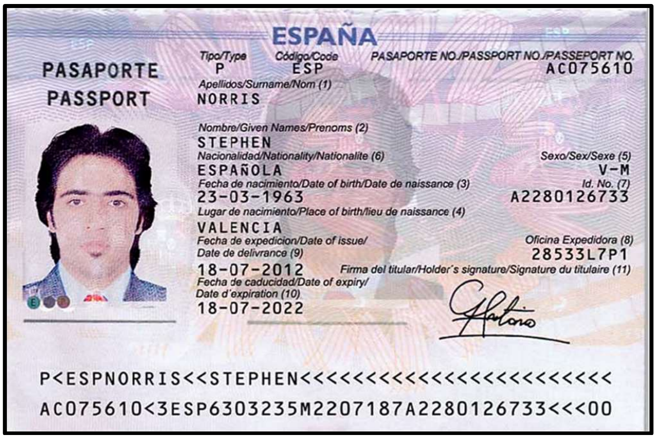
The attacker offers that he will split the amount of US$23.6M into a 50 % ratio for him and 50 % for us. The attacker requires the victim to act as a relative and the attacker will use his position as an attorney for the quick progress of the transaction and he stated that everything is legal. At this point, it is obvious that this is from the law point of view a financial fraud offer. So far, the attacker does not need any personal data or any other information; he just ascertains the possible interest and does not induce any time pressure.

Our positive response was followed by an email from the attacker with a recap of the previous communication and the attacker offered the option of filling out the needed documents to obtain the financial sum from the will. He requires personal information to confirm the identity of the victim (passport, driver's license, or any valid identification), phone number, contact address, occupation, and marital status; the attacker creates a slight time pressure.

After our negative response to share personal information, the attacker responds with appeals to the partnership, and assurances about the legality of the transaction; the personal information will not be misused. To promote confidence, the attacker encloses a copy of the passport, see Fig. 4. At this moment, we stopped the communication.

The period of the attackers' replies takes place in the afternoon of our time. The delay between replies varies between 2 to 9 days. Initially, the attacker responds quicker; later, with our unwillingness to share data, the attacker's motivation decreases. The attacker responds logically, orients himself in the communication, and refers to the previous communication. In the later stages of communication, the attacker makes substantive communication mistakes.

The attacker's language was at a good level throughout the communication. Invariable addresses, correct English style, and similar repetitive parts could be explained by the use of bots in communication. Also, the initialization of phishing and the response to the victim's first positive response could have been processed by robots. The parts of the communication where errors occurred are likely to have been processed manually.



ESPAÑA

PASAPORTE
PASSPORT

Tipo/Type P
Código/Code ESP
PASAPORTE NO./PASSPORT NO./PASSEPORT NO. AC075610

Apellidos/Surname/Nom (1)
NORRIS

Nombre/Given Names/Prenoms (2)
STEPHEN

Nacionalidad/Nationality/Nationalite (6)
ESPAÑOLA

Sexo/Sex/Sexe (5)
V-M

Fecha de nacimiento/Date of birth/Date de naissance (3)
23-03-1963

Id. No. (7)
A2280126733

Lugar de nacimiento/Place of birth/lieu de naissance (4)
VALENCIA

Fecha de expedicion/Date of issue/
Date de delivrance (9)
18-07-2012

Oficina Expedidora (8)
28533L7P1

Firma del titular/Holder´s signature/Signature du titulaire (11)

Fecha de caducidad/Date of expiry/
Date d'expiration (10)
18-07-2022

P<ESPNORRIS<<STEPHEN<<<<<<<<<<<<<<<<<<<<<<<<
AC075610<3ESP6303235M2207187A2280126733<<<00

Fig. 4 The passport of Mr. Norris

7 Security Policy, Education, and Defense Against Phishing Attacks

To ensure protection against phishing attacks, it is always necessary to provide basic security functions, which can be divided into security policy, trained personnel (training), and security measures (HW and SW). All of these security functions and their interdependence are important to successfully protect an organization against phishing threats and attacks.

7.1 Security Policy

Unfortunately, a large number of organizations live under the belief that sufficient protection can be provided by simply purchasing, i.e., acquiring firewalls, antivirus proactive features, etc. But this idea is completely wrong. Along with the development of information technology (IT), new opportunities for abuse are also emerging, which are linked not only to IT but also to their proper implementation, including the right security policy.

The security policy must respect primarily the security policy of the European Union (EU). The main document is Regulation 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cyber Security) [10] and on cyber certification security of information and communication technologies (ICT) and repealing Regulation No 526/2013 (Act on cybersecurity). The purpose of this Regulation is to set out the objectives, tasks, and organizational aspects relating to ENISA and establish a Framework for European cybersecurity certification schemes to ensure an appropriate level of cybersecurity of ICT products, services, and processes.

At the national level, the law is important in the area of cyber security. In the Czech Republic, it is the Act on Cyber Security, 181/2014 Coll. The Act regulates the rights and obligations of persons, as well as the powers and competencies of public authorities in the field of cyber security. It elaborates on the relevant EU regulations (it is a transposition of the NIS Directive) and regulates the provision of security of electronic communications networks and information systems.

7.2 Education

The education aspect is also very important. Phishing attacks have unfortunately become an integral part of our lives in recent years. For this reason, the issue of phishing attacks must be integrated into the education system, see Fig. 5.

Through quality education, there is a need to strengthen people's overall information literacy, responsibility, and resilience, which will also lead to an overall strengthening of cyber security. In the area of education, emphasis should be placed on projects that aim to teach skills in identifying phishing attacks, for example, in terms of unauthorized obtaining of sensitive user data, getting sensitive credit card information, or access to internet banking.

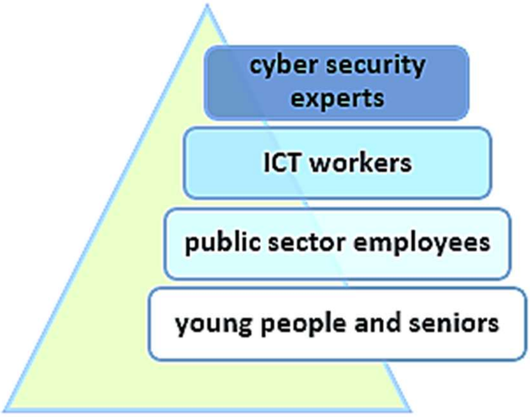


Fig. 5 Training of personnel in cyber security

In addition to educating young people, the focus should be on educating other selected target groups. This will include teachers and public administration employees. Teachers are a building block of the education system and their effective training in cyber security is essential for the development of information skills among pupils and students. The general understanding of digital hygiene, i.e. the set of principles, practices, and habits that enable users to move safely in virtual environments, varies widely among young people and needs to be targeted.

In terms of cybersecurity education, The National Cyber and Information Security Agency (NÚKIB) [11] has been very active, in preparing educational board games or interactive comics for young people. For students, the Czech branch of AFCEA organizes the High School Cybersecurity Competition. Public administration users were educated through the online course "Dávej kyber!" (Give Cyber!), which introduces the basics of cybersecurity. Educational activities for the general public are provided by the NÚKIB on its website. Great emphasis should also be placed on the development of ICT staff and experts in the field of cyber security.

The results of our research can be suitably used in the education of university students and the training of company and organization personnel in resistance to phishing attacks. When creating training materials and procedures, attention has to paid to the facts resulting from the analysis of phishing emails, for example, their predominant text in English. The results of the segmentation of phishing emails can be applied to the recognition of phishing texts. Keyword analysis of phishing emails can be used in the email filtering settings.

7.3 Anti-phishing Software Solutions

IRONSCALES

IRONSCALES [12] is currently one of the fastest-growing email security companies against phishing. Their solutions offer protection against advanced phishing email threats such as business email compromise, impersonation of VIPs, and Account Takeover. Their cloud-based solution is fully compatible with Microsoft Office 365 and Google Workspace. It uses artificial intelligence to provide real-time protection, which can be supplemented by an IT professional review.

The system protects against repetitive identical network intrusions. The system allows users to manually report suspicious emails using a button directly in their inbox (activation is possible on both PC and mobile). Following that report, other users who have received identical emails are also notified.

AVANAN

AVANAN [13] is a cloud security company that provides various cybersecurity solutions, including anti-phishing measures. Avanan's anti-phishing technology uses machine learning and other advanced techniques to identify and block phishing attacks before they reach users. The technology analyzes emails, URLs, and other digital assets in real-time to identify suspicious activity and patterns that may indicate phishing attempts.

This anti-phishing solution also includes user-awareness training to help educate employees on how to recognize and avoid phishing attacks. By combining advanced technology and user education, it provides a comprehensive anti-phishing solution that helps organizations protect themselves from this common and dangerous form of cyberattack.

ABNORMAL SECURITY

ABNORMAL SECURITY [14] is a cloud-based email security platform that provides advanced anti-phishing measures using artificial intelligence and machine learning. It is designed to help businesses of all sizes protect themselves from sophisticated phishing attacks that traditional security systems cannot identify.

Abnormal Security uses behavioral analytics to identify and block phishing emails in real time, as well as machine learning algorithms to identify and block advanced phishing attacks that may contain zero-day exploits. It also provides email security features such as URL protection, attachment scanning, and sender reputation analysis.

One of the key features of Abnormal Security's anti-phishing solution is the use of social graphs that analyze the relationships between email senders and recipients to identify potential phishing attempts. It also uses natural language processing and computer vision to analyze the content of emails and detect social engineering tactics used in phishing attacks. Abnormal Security's anti-phishing solution is integrated into Microsoft Office 365 and Google Workspace.

8 Conclusions

The article presents a comprehensive study of phishing attacks. The analyzed data was obtained from the university mailbox of one of the authors. The research was carried out in several experiments to recognize phishing emails and find out the typical behavior of a phishing attacker. The experiments carried out were evaluated using analytical methods and processed using the text-analytical SW Tovek. The results achieved have been verified. All acquired knowledge will be used primarily in the teaching of university students. The research is original, no similar study has been found in the literature.

Acknowledgment

The article presents the results of the research project KYBERSILY [15].

References

[1] SLIFKIN, E.J.D. and M.B. NEIDER. Phishing Interrupted: The Impact of Task Interruptions on Phishing Email Classification. *International Journal of Human-Computer Studies,* 2023, **14**, 103017. DOI 10.1016/j.ijhcs.2023.103017.

[2] TAN, C.C.L., K.L. CHIEW, K.S.C. YONG, Y. SEBASTIAN, J.C. THAN and W.K. TIONG. Hybrid Phishing Detection Using Joint Visual and Textual Identity. *Expert Systems with Applications*, 2023, **220**, 119723. DOI 10.1016/j.ijhcs.2023.103017.

[3] VISHWANATH A., T. HERATH, R. CHEN, J. WANG and H.R. RAO. Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability Within an Integrated, Information Processing Model. *Decision Support Systems*, 2011, **51**(3), pp. 576-586. DOI 10.1016/j.dss.2011.03.002.

[4] ALSHARNOUBY, M., F. ALACA and S. CHIASSON. Why Phishing Still Works: User Strategies for Combating Phishing Attacks. *International Journal of Human-Computer Studies,* 2015, **82**, pp. 69-82. DOI 10.1016/j.ijhcs.2015.05.005.

[5] ABBASI, A., F. ZAHEDI and Y. CHEN. Impact of Anti-Phishing Tool Performance on Attack Success Rates. In: *2012 IEEE International Conference on Intelligence and Security Informatics*. Washington: IEEE, 2012. DOI 10.1109/ISI.2012.6282648.

[6] TURČANÍK, M. Behavior Analysis of Web Users by Mean Shift Clustering. In: *2021 International Conference on Military Technologies (ICMT)*. Brno: IEEE, 2021, pp. 1-6. DOI 10.1109/ICMT52455.2021.9502771.

[7] TURČANÍK, M. Web Users Clustering by their Behavior on the Network. In: *2020 New Trends in Signal Processing (NTSP)*, Demanovska Dolina: IEEE, 2020, pp. 1-5. DOI 10.1109/NTSP49686.2020.9229548.

[8] TURČANÍK, M. Using the Recurrent Neural Network for Hash Function Generation. In: *2017 International Conference on Applied Electronics (AE)*. Pilsen: IEEE, 2017, pp. 1-4. DOI 10.23919/AE.2017.8053625.

[9] *Software and Information Sources of the Company TOVEK* [online]. [viewed 2023-11-12]. Available from: www.tovek.cz

[10] *ENISA Mandate and Regulatory Framework* [online]. [viewed 2023-11-15]. Available from: https://www.enisa.europa.eu/about-enisa/regulatory-framework

[11] *NÚKIB, Education* [online]. [viewed 2023-11-01]. Available from: https://nukib.gov.cz/en/cyber-security/education/

[12] *IRONSCALES* [online]. [viewed 2023-11-09]. Available from: https://ironscales.com/

[13] *AVANAN* [online]. [viewed 2023-10-26]. Available from: https://www.avanan.com/

[14] *ABNORMAL SECURITY* [online]. [viewed 2023-10-26]. Available: https://abnormalsecurity.com/

[15] DZRO-209, University Research Project KYBERSILY: Cyber Forces and Assets, Brno, University of Defence, 2021-2025.