How to Understand Phishing

LADISLAV BURITA
Department of Informatics and Cyber Operations,
University of Defence,
65, Kounicova Street, 662 10 Brno,
CZECH REPUBLIC

Abstract: - The article is based on the results of previous research, is focused on the analysis and classification of phishing emails, and documents the results of communication with the phisher attacker. In the first part of the article, an experiment carried out with a randomly selected set of emails confirms the considerable uncertainty of the correct result of automatic classification based on keywords using text analysis software. The second part of the article contains the experiment of communication with phishing attackers. A typical scenario of message exchange is presented. Thanks to the correct setting of security and protection rules, no security incident occurred. The literature search confirms the great interest in publishing in the field of phishing. Compared to the content of the published article, it turned out that its focus is completely original.

Key-Words: - Phishing, email, analysis, classification, phisher, communication

Received: February 17, 2022. Revised: November 12, 2022. Accepted: December 7, 2022. Published: January 9, 2023.

1 Introduction

The article deals with several aspects of email phishing, clarifies their threats and attacks, analyzes the content of phishing messages, and gives instructions on communicating with a phishing attacker without risk. It summarizes the research results the author has been working on for several years.

Everyone who uses e-mail has probably encountered phishing, knowingly or unknowingly; many of the users failed to respond properly to the phishing attack and fell victim to it.

Let us first state one of the many possible definitions of phishing as it is given in the Cyber Security Dictionary, published under the auspices of The National Cyber and Information Security Agency of the Czech Republic [1]: "*Fraudulent methods have the objective of stealing the digital identity of a user, the sign-on names, passwords, bank account numbers, and accounts, etc. in order to subsequently misuse these (drawing cash from the account, unauthorized access to data, etc). Creation of a fraudulent message distributed mostly by electronic mail trying to elicit the mentioned data from the user. The messages may be masqueraded so as to closely imitate a trustworthy sender. It may be a forged request from a bank whose services the user accesses with a request to send the account number and PIN for a routine check (use of the dialog window purporting to be a bank window – so-called spoofing). Thus the fraudster tries to convince accessing persons that they are at the right address whose security they trust (pages of electronic shops etc.). Also, very often credit card numbers and PINS are stolen in this fashion*."

It can be assumed that we all have savings accounts in the bank. Fraudsters are always looking for ways to get their hands on your money. Most often, they try it through emails, SMS messages, phone calls, social networks, fake websites, and payment gateways. Banks warn against fraudsters, inform about possible forms of fraud, and give advice on how to recognize fraud [2]:

- The message or call is very urgent and calls for your immediate response. The fraudster can pretend to be a bank, a government institution, a seller, or a buyer.
- The fraudster redirects you to his fake website, where he requests your account login or card details and thereby steals them.
- The most common excuses are, for example, blocking of an account, card, or access to banking for your safety, payment of a long unpaid debt with the threat of execution, checking of received payment in banking via the sent link, etc.

Of course, the bank also advises how to protect yourself [2]:

- Never sign up via sent links.
- Do not search for the bank's website through any search engine.

- Always read the texts of the certification and confirmation messages carefully! By confirming, you approve a fundamental and irreversible action.
- Before entering payment card details, first, make sure of the authenticity of the site. Always check the amount and merchant name when paying.

There are enough research works on the phishing themes, as described in Chapter 2. A more detailed analysis of literary sources was focused on the classification of phishing emails and communication with a phisher.

The article is organized as follows; the Introduction, the Methodology and Used Tool, and Literary Review.

The article's core is a Chapter on the Analysis and Segmentation of Phishing Emails with a Chapter on Communication with a Phisher; the last part is Conclusions and References.

2 Methodology and Used Tools

The source for phishing analysis is emails sent to the paper's author. Every email was stored as a single file. It takes about several hundred emails; every month of the experiments some tenths.

A sample of 50 emails for the paper was randomly selected from those files. The data set was an object for content analysis with respect to the results of previous experiments.

The goal of content analysis is phishing email segmentation using the text analytical SW Tovek. Keywords for segmentation are carried out on the basis of selected relevant keywords from previous research.

The result of the segmentation (segment Business, Fund, Transfer, Charity, and Others) was correlated using the Tovek context analysis. SW Tovek [3] enables indexing of source files; effective simple and complex search; contextual, and content analysis.

For the chapter dedicated to communication with a phishing attacker, emails were chosen primarily from the Others segment in order to achieve a greater number of email exchanges. The typical content of the communication is shown by a sequential UML diagram. UML (Unified Modeling Language) is a general tool for system and process modeling; the model was created in SW Enterprise Architect [4].

The result of the literature review is compared with the goals of the paper.

3 The Literature Review

The literature review was oriented to the documents indexed in Scopus [5] using the keywords “phishing, email, analysis, research, communication” selected 14 articles. Their focus was on:

- Detection of phishing messages and defense against them [6], [7], [8], and [9].
- Vulnerabilities of users to phishing attacks and their education [10], [11], and [12].
- Classification of phishing emails [13], [14], [15], and [16].
- Phishing research in connection with malware, Blockchain, and botnet [17], [18], and [19].

In relation to the orientation of the publication, articles in the literature review dealing with the classification of phishing messages will be further discussed.

An overview study [13] on the content and development of phishing spam deals with the analysis of analytical disciplines for the recognition and classification of spam. Lists classification techniques:

- Supervised Machine Learning.
- Unsupervised Machine Learning.
- Semi-supervised Machine Learning.
- Content-based Learning.
- Statistical Learning.

The study contains an analysis of literary sources in the areas of:

- Identification of Spam Classification Application Areas.
- Spam Classification Dataset Analysis and Review.
- Feature Set Analysis and Review.
- Spam Classification Techniques Analysis and Review.
- Performance Metrics Review and Analysis.

Paper [14] is oriented to the legal analysis of phishing emails; this is completely original research. Emails were acquired via two email accounts in the period of one month (a total number of 297 emails).

The emails were assessed from the point of view of legal rules: header and subject line, greetings, body text, and instructions to the recipient.

The classification was made according to the RIFE (Robbery, Informational, Fraud, Extortion) scale of influence and impact on the will to act.

As a result of the classification, the selected emails were marked as:

- Fraud (29 cases).
- Extortion (3 cases).

- Personal data processing-related misdemeanor offenses committed (10 cases).

The book chapter [15] is focused on examining phishing emails as a business scam. Phisher offers a business partnership using email with the goal of defrauding the recipient of the message. Another example of phishing emails in business seeking assistance to transfer or claim money from bank accounts. The analysis also highlights the rhetoric and persuasive strategies of email phishers using interpersonal relationships in negotiation, trust, and confidentiality. The study concludes that email business scams will continue in the future because the phishers not only demonstrate competence in communication, but they also take information technology to the fullest. In addition, they abuse human interest to get free money.

The review [16] deals with email classification, and uses the general architecture of automatic classification that is divided into three distinct levels: pre-processing, learning, and classification. The source for research is articles from WoS and Scopus in the years 2006 – 2016 (a total of 98 articles selected), from which clear tables are compiled, in which applied methods are analyzed in detail. Application areas in email classification consist of five areas: spam, phishing, spam and phishing, multi-folder categorization, and others.

The literary source [13] discusses methods and techniques of classification, it does not specify the particular classification of phishing emails. It is a motivation paper for the choice of suitable methods and techniques for phishing research.

The method of data collection in the study [14] is the same as the data collection in our previous research stages (the number of phishing emails also roughly corresponds). Regarding the classification of phishing emails, one can exaggeratedly assign Fraud emails to the Fund segment and Extortion to the Transfer segment; if we do not take into consideration legal aspects Personal data was the target of the emails of most segments.

Document [15] contains the classification of phishing emails and recognizes the segment Business, and Transfer, which is in accordance with the findings in Chapter 4 of the article.

The review [16] has a much wider scope than our article, which is devoted to the application level of the phishing classification.

4 Analysis and Segmentation of Phishing Emails

The chapter deals with the analysis and segmentation of a set of 50 phishing emails selected (by size). The segmentation process is carried out using the text-analytical SW Tovek, based on 5 typical keywords obtained from previous research for the segment:

- **Business:** business, project, invest, contract, employment.
- **Fund:** fund, compensation, prize, gift, inheritance.
- **Transfer:** transfer, bank, shipment, money, gold.
- **Charity:** charity, cancer, hospital, widow, Christ.
- **Others**: contact, loan, undelivered, package, shipment.

The user interface of SW Tovek in segmentation (Business) is in Fig. 1.

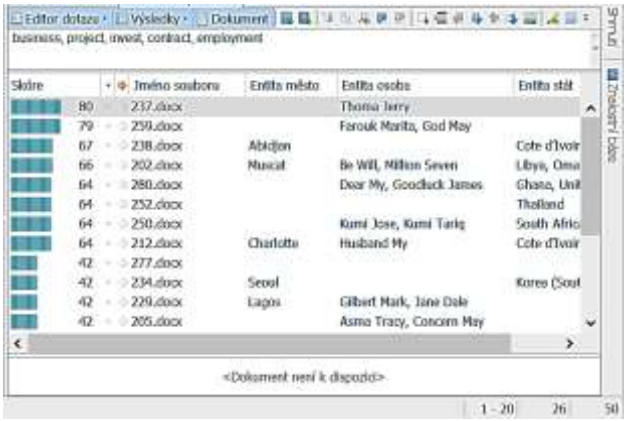

Fig. 1: The user interface of the SW Tovek

The result of the operation places emails into individual segments as follows: Business (26), Fund (30), Transfer (28), Charity (11), and Others (35); a total of 130 emails were selected, which is much more than the analyzed 50 emails.

The problem is that keywords are spread throughout emails regardless of segmentation. So the automatic analysis fails and needs to be fixed "manually".

How keywords are spread out in emails is shown by the result of the context analysis, see Fig. 2. In each node of the context matrix, the number of emails containing keywords from the intersection of the segments is listed.

For example, the segment Transfer and Charity have 6 emails in common (they contain keywords from both segments). It can be displayed in a set of emails, see Fig. 3 and analyze individual emails. For example, file 239 includes the keyword "cancer"

from the Charity segment and the word "money" from the Transfer segment:

It's important: Sorry for intruding into your privacy. My name is Nicole Marois Benoite from (Paris) France Married to Terry Benoite. I am currently ill with cancer disease and I wish to donate my inheritance ($4.5 MILLION DOLLARS) that my late husband left with a financial institution. My doctor told me that I have just a few days to leave due to my cancer illness. I want you to help me use this money for the less privileged in your country. Reply me back immediately so that I will give you more details only if you are willing and ready to handle this project. Best Regards Nicole Marois Benoite.

Remarque to email 239: In addition to keywords, the so-called entities (numbers, names, countries, cities) are highlighted colourfully.

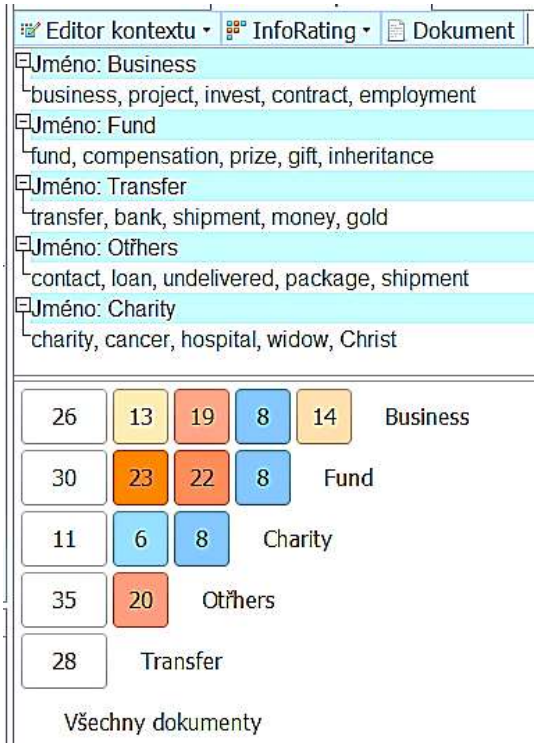

Fig. 2: The context matrix of segmentation

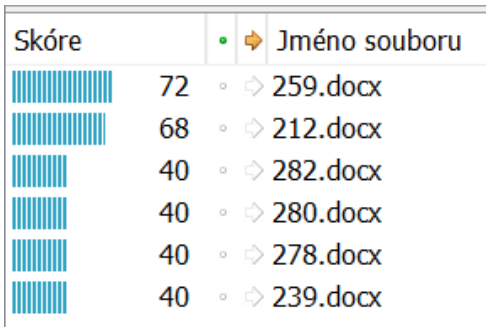

Fig. 3: Files of node Charity - Transfer

The result of “manual” segmentation correction is as follows: Business (12), Fund (18), Transfer (11), Charity (6), and Others (3).

The differences between the automatic and manual classification of phishing emails are significant, therefore only manual classification can be recommended as a default method, and automatic classification only as an auxiliary method to clarify hidden contexts.

5 Communication with a Phisher

The goal of communicating with the phishing attackers was to find out more precisely how that communication can take place and how the phisher may argue to get the required information.

For safe communication with the phisher, it is necessary to accept and follow security and protection rules. Communication took place via fake identity, fundamentally outside the university network.

The initial phisher email was transferred from the author's email account to the fake identity's email account and sent with a response selected from a pre-prepared set of reactions.

A suitable email for communication is one that has indefinite content.

Further communication was already taking place via the fake identity account, its progress was recorded for later detailed analysis. Typical communication includes steps (see Fig. 4):

1. An email with an unspecified requirement.
2. Query to clarify the request.
3. A message with the targeted requirement.
4. Request for a more detailed explanation.
5. A detailed message was sent.
6. Expression of no confidence in the message.
7. Another phisher argumentation.
8. Termination of communication.

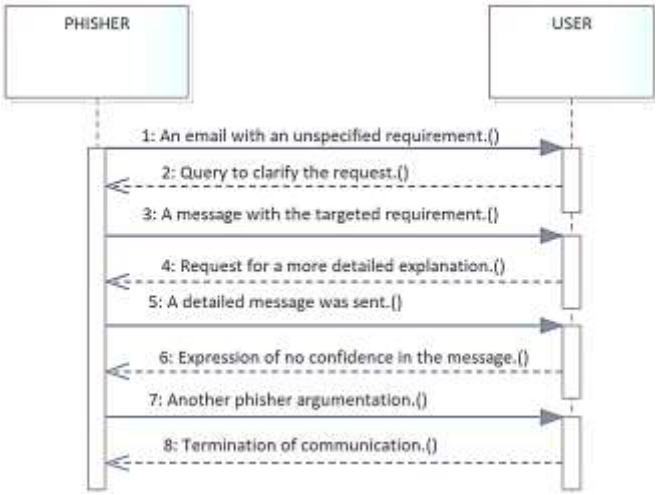

Fig. 4: Communication with a phisher

Examples of **an email with an unspecified requirement:**

- I trust that all is well with you and your family. Did you receive my previous email?
- You were chosen by God to receive my Grant Donation of $1.2M. Please contact me via email:
- I have a profitable and risk-free deal for you. Contact me if you are willing to know more.
- I would like to disclose something very important to you, get back for more details.
- Please, I want to discuss a profitable financial deal with you.
- Donation of 500.000 GBP.
- I would like to disclose something very important to you, get back for more details.
- Your reputable profile gives me the impression that you will be a suitable partner in a crude oil licensing operations venture. Upon your response, I will give you clearer details of this operation.

Examples of **the query to clarify the request:**

- Sorry, but I did not receive your previous email. What is it about?
- Thank you for the Grant Donation.
- Inform me please about the mentioned business in detail, please.
- Would you be kind enough to explain what it is about to me?
- I am interested in your offer. Could you inform me in detail?
- Inform me how to get the mentioned donation, please.
- Would you be kind enough to explain what it is about to me?
- Inform me more in detail, please.

A message with the targeted requirement contained a description of the phisher's proposal (most often from the segment Fund, Business, and Transfer) and requirements for sending personal data.

Examples of **another phisher argumentation**:

- Above all, other "credible" details of the previous proposal.
- A copy of the identity card or passport of the phisher.
- A photograph proving the personality of the communicator.
- Redirection to the next participant in the communication (lawyer, banker, assistant).

It is necessary to add with satisfaction that there was no safety incident during the experiment. The result fully clarified the phisher's way of communication, so it is possible to better defend against phishing threats and attacks based on the information obtained.

6 Conclusion

The article is focused on understanding phishing emails. The first experiment with automatic email segmentation based on selected keywords confirmed the low reliability of this method.

It can only be applied as a supportive tool; it is necessary to rely on "manual" classification. Keywords are placed in multiple emails, regardless of their focus in favor of a certain segment classification. The results of both approaches in the experiment are quite different.

The second experiment verifies communication with phishing attackers. There was no security incident when the protection and security rules were followed. Lessons learned from communicating with a phisher explain the way the phisher communicates and argues in order to convince you of the legitimacy of his request. No lie is good enough for him.

Future research could be oriented more to the education of users in resistance against the phishing threats and attacks.

References:

[1] Jirasek, P., Novak, L. and Pozar, J., *Cyber Security Glossary, the fifth supplemented and revised edition*, published under the auspices of The National Cyber and Information Security Agency of the Czech Republic, 2022.

[2] Raiffeisenbank: Safe banking, what is phishing, and how to protect yourself, Available at https://www.rb.cz/bezpecne-bankovnictvi/phishing
[3] Tovek Company. Available at https://tovek.cz/
[4] Sparx Systems Company: Enterprise Architect, Available at https://sparxsystems.com/
[5] Scopus: Document search, Available at https://www.scopus.com/search/form.uri?display=basic#basic
[6] Kadir, M.F.A., Abidin, A.F.A., Mohamed, M.A., and Hamid, N.A., Spam detection by using machine learning based binary classifier, *Indonesian Journal of Electrical Engineering and Computer Science*, 26(1), pp. 310-317, 2022.
[7] Bhattacharya, M., Roy, S., Chattopadhyay, S., Das, A.K., and Jamal, S.S., ASPA-MOSN: An Efficient User Authentication Scheme for Phishing Attack Detection in Mobile Online Social Networks, *IEEE Systems Journal*, pp. 1-12, 2022.
[8] Livara, A., and Hernandez, R., An Empirical Analysis of Machine Learning Techniques in Phishing E-mail detection, *International Conference for Advancement in Technology*, ICONAT 2022.
[9] Varshney, G., Misra, M., and Atrey, P.K., A survey and classification of web phishing detection schemes, *Security and Communication Networks*, 9(18), pp. 6266-6284, 2016.
[10] Xu, T., Singh, K., and Rajivan, P., Personalized persuasion: Quantifying susceptibility to information exploitation in spear-phishing attacks, *Applied Ergonomics*, 108,103908, 2023.
[11] Jampen, D., Gür, G., Sutter, T., and Tellenbach, B., Don't click: towards an effective anti-phishing training. A comparative literature review, *Human-centric Computing and Information Sciences*, 10(1), 33, 2020.
[12] Ferreira, A., and Teles, S., Persuasion: How phishing emails can influence users and bypass security measures, *International Journal of Human Computer Studies*, 125, pp. 19-31, 2020.
[13] Abari, O.J., Sani, N.F.M., Khalid, F., Sharum, M.Y.B., and Ariffin, N.A.M., Phishing Image Spam Classification Research Trends: Survey and Open Issues, *International Journal of Advanced Computer Science and Applications*, 11(11), pp. 794-805, 2020.
[14] Kikerpill, K., and Siibak, A., Living in a spamster's paradise: Deceit and threats in phishing emails, *Masaryk University Journal of Law and Technology*, 13(1), pp. 45-66, 2019.
[15] Chiluwa, I.M., Chiluwa, I.E., and Ajiboye, E., *Online deception: A discourse study of email business scams (Book Chapter)*, Deception and Deceptive Communication: Motivations, Recognition Techniques and Behavioral Control, pp. 169-188, 2017.Mujtaba, G., Shuib, L., Raj, R.G., Majeed, N., and Al-Garadi, M.A., Email Classification Research Trends: Review and Open Issues, *IEEE Access*, 5,7921698, pp. 9044-9064, 2017.
[16] Vance, T.R., and Vance, A., Cybersecurity in the blockchain era: A survey on examining critical infrastructure protection with blockchain-based technology, *IEEE International Scientific-Practical Conference: Problems of Infocommunications Science*, 2019.
[17] Qbeitah, M.A., and Aldwairi, M., Dynamic malware analysis of phishing emails, *9th International Conference on Information and Communication Systems*, pp. 18-24, ICICS 2018.
[18] Ilavarasan, E., and Muthumanickam, K., A Survey on host-based Botnet identification, *International Conference on Radar, Communication and Computing*, 6450569, pp. 166-170, ICRCC 2012.
[19] DZRO FVT 2_KYBERSILY, Research project Cyber forces, and resources, University of Defence, Faculty of Military Technology, Brno, Czech Republic, 2022.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)
The author contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself
No funding was received for conducting this study.

Conflict of Interest
The author has no conflict of interest to declare that is relevant to the content of this article.