

UDC 004.056:004.89

## **Peculiarities of phishing threats and preventive measures in the conditions of war in Ukraine**

Hryhorii Shevchenko<sup>1</sup>, Iryna Stopochkina<sup>2</sup> and Ivan Babenko<sup>3</sup>

<sup>1,2,3</sup> *National Technical University of Ukraine "Igor Sikorsky KPI",  
Peremogy ave., 37, Kyiv, 03056, Ukraine*

---

### **Abstract**

The paper is devoted to the study of the peculiarities of phishing attacks on the personnel of enterprises and institutions of Ukraine during the war period (from February 2022- till now). The life cycle of the most popular attacks is analyzed. The focus is made on email phishing, which is the most popular for attacks on enterprises. A list of typical topics of phishing emails, psychological vectors of phishing influence, typical for attacks on Ukrainian users, additional factors that contribute to the success of attacks have been revealed. A countermeasures for phishing attacks prevention have been recommended. A list of phishing keywords was collected and templates were developed, a software solution based on artificial intelligence approaches was proposed to automate the generation of phishing letters in Ukrainian that can be used during "false alarms" and staff training in large enterprises.

*Keywords:* Phishing, War in Ukraine, CyberThreats, Countermeasures

---

### **Introduction**

Cyber attacks using phishing are often used by criminals. The growing popularity of phishing attacks is illustrated by analytical reports on cyber security. Researchers from Blackfog, Anomali, Coresecurity, and Acronis report that phishing ranks first among the cyberthreats most used by criminals. The factors that determine the success of phishing are the prevalence of access to the Internet, mail services and messengers, the practice of publishing information available to the general public in social networks, etc. Company employees almost always have access to work e-mail, where information about upcoming meetings, new tasks, etc. is received. Therefore, phishing can still be extremely effective for deception, obtaining the necessary information for other attacks. According to [1], the following most common types of attacks are highlighted: 1) bulk phishing, 2) spear phishing, whaling, 3) business e-mail compromise attacks 4) e-mail based ransomware attacks, 5) attacks via social media, 6) smishing, 7) vishing, 8) malicious USB drops.

The analytical report [2] noted that the total number of phishing attacks for the year (from May 2021 to April 2022) reached 1,122,579 attacks (+426,756), and actually increased twice as compared to May 2020. Quarterly reports from the Anti-Phishing Working Group [3] over the past few years also show a steady and significant increase in the number of phishing attacks, despite investment in security measures. An analysis of own secure email gateway statistics of one of the financial institutions of Ukraine also shows a significant increase in the number of phishing attacks (329 cases in 2021 versus 538 in the first 8 months of 2022). This is due to the fact that phishing attacks use new technologies (Phishing-as-a-service), which significantly lowers the threshold for entering the phishing business, as well as the fact that they use not only technical means, but are based in largely on the peculiarities of human psychology. Unprepared employees can be tricked into clicking on a malicious link in an email, fall victim to a malicious redirect, or tricked into a hacker-controlled copy of a website. Attackers use a variety of tactics to launch phishing attacks against their targets, including emails, fake pages and fake social media identities, sms, instant

messages, and compromised websites. Consequently, phishing continues to be the biggest threat to large and small organizations as it is difficult to keep up with all the new social engineering trends. In addition, the next generation of phishing attacks can be carried out using artificial intelligence approaches, which can multiply the possibilities of creating phishing emails. This raises new challenges aimed at increasing the readiness of enterprise personnel.

The preparedness of citizens for social engineering attacks in conditions of unfavorable social and psychological factors is especially important. In particular, in the conditions of war and terror against the population of Ukraine by the aggressor country.

In Ukraine, during the armed aggression of Russia, a significant number of institutions and enterprises were subjected to Russian cyber attacks, which were based, including, on phishing techniques [4].

This work presents an analysis of the features and reasons for the success of phishing attacks on Ukrainian institutions during wartime, and provides recommendations for prevention and protection against these attacks. Attention is focused on attacks that occur through e-mail, due to the fact that this is the most typical way of influencing an employee of an enterprise during the performance of his official duties. The typical lifecycle of phishing attacks were presented. The practical problem that was solved in the paper is an automated solution that can be used in training vigilance and awareness of personnel of large enterprises. The improved phishing text generator can be used for large enterprises staff awareness training.

## **1. Attack lifecycle definition**

Determining the life cycle of a particular social engineering attack is quite complex because each attack involves people with their behavioral changes over time, as well as their mood and other personal or emotional characteristics.

Nevertheless, four stages of a social engineering attack have been identified [5]: research (collection of information), development of relationship and trust, use of trust and use of information. One cycle is not necessarily limited to a single iteration, but may contain several iterations until the goal is achieved [6]. Therefore, the process itself can be

recursive and iterative, depending on the attack and the methods used:

1) Gathering information - this stage consists of several methods of obtaining a significant amount of information about the victim. Different methods can be used depending on whether the phisher's victim is a company or an individual. The ultimate goal of this stage is to obtain as much information as possible about the target to further develop the relationship, interaction and trust for the next stage.

2) Development of relations - at this stage, the social engineer makes contact through the means of communication available to him. The attacker uses methods of establishing trust, for example, referring to the names of verified employees or individuals, using professional slang, demonstrating familiarity with the business process, demonstrating shared values. As soon as the criminal feels that the necessary degree of trust has been achieved, he moves on to the next stage.

3) Exploitation of relationships – after establishing communication and trust, the criminal uses the opportunity to influence the victim by inventing a story that affects the emotional and psychological state of the victim, the peculiarities of his behavior in unusual conditions, in particular when there is a lack of time to perform urgent tasks, force majeure circumstances, atypical situations that require a reaction.

4) Use of information – at this stage, the information or the actions of provoked victim are used to carry out an attack with or without the use of technical means or to use the obtained information for a new socially engineered attack. With the help of this stage, the attacker achieves the desired goal (for example, unauthorized access to the information object, compromising the victim, undermining the reputation of the enterprise, infection with malicious software for the purpose of destroying information objects, etc.).

In [6] it is justified that most of the weak points that are exploited by attackers are common to many companies. It is also argued that even the best technical mechanisms do not prevent attackers in most cases. And even if the attackers were unable to gain unauthorized access to the information system, they can still obtain sensitive personal or corporate information.

In addition, security operators must take into account the non-technical side of computer

security and not assume that software and hardware tools are sufficient to prevent social engineering attacks. In addition, computer specialists very often believe that the basics of computer security are known to everyone, but this is not true [7]. Most authors consider increasing user awareness and regular staff training as an important part of countering social engineering, but this can only reduce the risks in this area, but not completely get rid of them.

Regarding those typical attacks carried out in Ukraine since January 2022, the following can be noted:

- Most of these attacks were of a simplified nature, when the phase of establishing trust relations is combined with the attack phase. An email is immediately sent with a certain offer, which should interest the victim, arouse his trust, and provoke him to take certain actions that are beneficial to the attacker (for example, click on a link, open an attachment, transfer funds).
- Publicly known e-mail addresses were used; contacts published by organizations on their web resources; or, presumably, the addresses are set by brute forcing through possible values (for example, using <http://metricsparrow.com/toolkit/email-permutator/> for possible addresses generation, knowing name, nickname and surname of the victim). If these are gmail addresses, it is not necessary to do mass mailings, the attacker can easily establish the activity of the address (simply by entering it to send mail in the Gmail service).
- The Gmail account shows a photo of the person (if it is present), by which the age can be determined (for example, using <https://howolddoyoulook.com/>), which will give the phisher more information about the psychological characteristics of the person.
- Some smartphones give the photo with metadata (geolocation), then it posted in social networks, and phisher could investigate, where the photo was made. Also sun shadows and time, fixed on photo, can give an information about geolocation, where the photo was made.
- For spear phishing and whaling, additional intelligence is conducted by searching through open sources of information (OSINT) about the target person. Open posts on Facebook, LinkedIn, Twitter contribute to this. A profile of communication

with a person is established based on the DISC model [8]. The profiling can be done even by photos in open access.

- An attacker, by intercepting the 2nd authentication factor, can gain access to the victim's resources, using a reverse proxy server, in this way - obtain complete information about the person posted on the resource [9]. Such attacks can be successfully carried out, for example, for Twitter, and for some mail providers.

For reconnaissance and targeted phishing, attackers can use the questionnaire method, introducing "anonymous" polls, or questionnaires with typical social engineering questions about a person:

- What accounts in social networks does he use?
- What hobbies does he/she have?
- Where does a person rest?
- What is the person's level of education?
- Where he/she works?
- From home, for himself, and to whom does he/she report?
- Are there other sites on which the person is mentioned (Speeches, posts, membership in clubs, comments on social networks, forums).
- Does the person own a house/apartment/car.
- Loans, pledges, etc.?
- What are the names of a person's family members?

Often, such surveys look like sociological or marketing research, and in Ukraine they can be found, for example, during "anonymous" questionnaires in shopping centers for participation in promotions or raffles, or as quizzes in social networks. The agency method of obtaining information about the target person, through a circle of acquaintances and relatives, is widely used.

There are also cases of leakage of databases with personal information of citizens that are accessible on darknet resources. These resources can be an additional source of information for phishers.

The lifecycle of targeted (spear) phishing typical attack is shown in Fig.1, and the shortened lifecycle of more simple bulk phishing attack is shown in Fig.2.

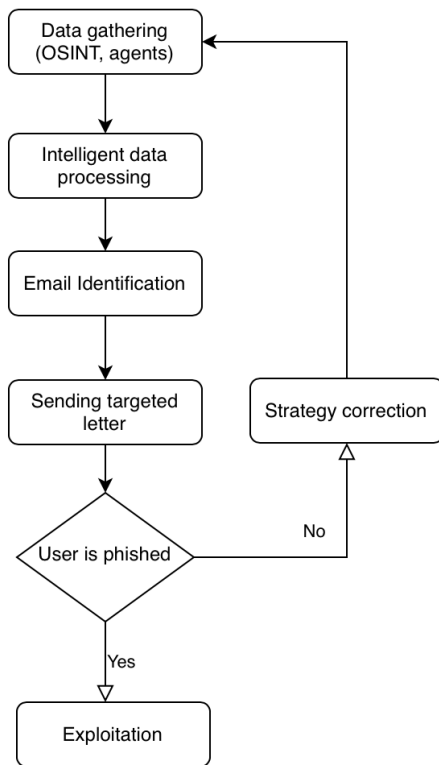


Figure 1: Typical spear phishing attack lifecycle

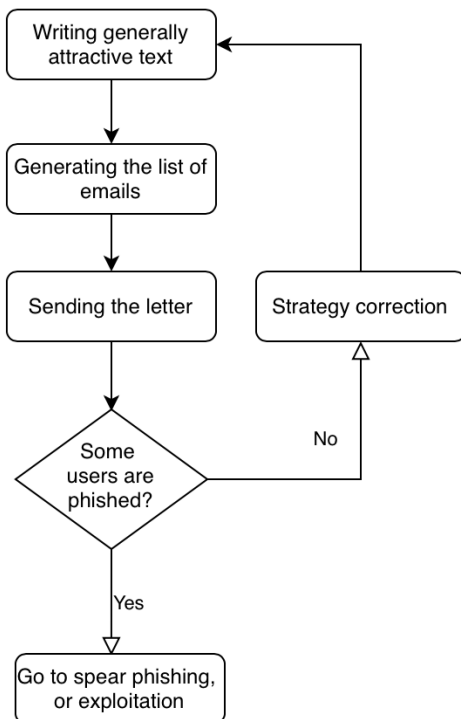


Figure 2: Bulk phishing attack lifecycle

A typical channel used to phish officials is email. Therefore, in the future, we will consider cases of phishing by sending an e-mail.

## 1.1. Typical topics of phishing letters

Typical topics of phishing emails for the Ukrainian sector from the beginning of February 2022 refer directly to military events:

- donation for the Armed Forces of Ukraine;
- news of military events;
- help to volunteers;
- donation for displaced persons;
- attention: chemical/biological threat;
- how to save yourself during a nuclear threat: instructions for actions;
- collection of signatures for consideration of the draft law (which will improve the situation of soldiers of the Armed Forces, Territorial Defense, etc.);
- collecting signatures to attract the attention of the community abroad (regarding the need for assistance to Ukraine);
- updated schedule of power outages.

For example, the UAC-0010 (Armageddon) group, which is linked to the FSB of Russia, according to CERT-UA, during the war used the following topics of e-mails, or file names and links in them to make an emotional impact:

"IT tools that have an expert opinion on compliance with the requirements of technical information protection" (November 2022);

"Combat order" (July 2022);

"Information bulletin of the Counterintelligence Department of the Security Service of Ukraine dated July 22, 2022" (July 2022);

"Regarding the revenge action in Kherson!" (May 2022);

"Regarding the facts of persecution and killing of Prosecutor's Office employees by the Russian military in the temporarily occupied territories" (April 2022);

"List of necessary things for the provision of military humanitarian assistance to Ukraine" (April 2022, attack on the state institutions of the countries of the European Union);

"Providing military humanitarian assistance to Ukraine" (April 2022, attack on state institutions of European Union countries);

"Information on war criminals of the Russian Federation" (April 2022).

Also topics typical for phishing emails can be used [9]:

- you have received payment/or gift;
- you received the package;

- unusual activity in your account;
- advertising newsletter, if you wish to unsubscribe, follow the link;
- meeting for employees;
- urgent work task;
- your password has been successfully reset;
- urgent complaint from the client.

As a rule, such letters contain attachments, inside which links to malicious resources are provided, the transition to which activates the attack. Or, such a link can be contained in the text of the letter. This tactic allows to pass the check of protection tools that do not check the links located in the letter, and becomes more and more used.

Also, the file attached to the email may be infected with malware.

Such letters often contain errors, poor Ukrainian language with incorrectly used words, atypical constructions. This may indicate the use of automated translation, for example, from Russian. The letters may contain facts that are difficult or impossible to verify, and, at the same time, require immediate action.

The following are the psychological vectors of attacks against Ukrainians:

1. Desire to help;
2. Fear, anxiety;
3. Inattention;
4. Curiosity;
5. Greed;
6. Irritation.

Vectors 1,2,6 play the main role under war conditions.

The types of phishing used in the largest attacks are targeted phishing; fictitious appeals on behalf of the Security Service of Ukraine, the Ministry of Defense of Ukraine, representatives of the Armed Forces of Ukraine, city administrations, volunteers. A large number of emails from suspicious domains are successfully blocked by mail filters.

## **1.2. Scope of phishing attacks on Ukrainians in the period from February 2022 to now**

According to the list of registered successful attacks using phishing in various spheres of activity, the following main sectors of attacks in Ukraine can be distinguished [4]:

- energy;
- civilians;
- public administration;
- media;
- financial sector.

### **1.2.1. Additional success factors for attacks**

Additional factors in the success of phishing attacks are the unfavorable conditions of personnel working with e-mail:

- Fatigue;
- A state of constant stress and nervous tension;
- Inattention;
- Ignorance of the features and possible consequences of phishing;
- Lack of sources where the facts can be approved;
- Lack of interaction with the information security department;
- Absence of job instructions on safe viewing of work correspondence;
- Lack of time to analyze events.

Phishing-As-A-Service type resources provide opportunities to use pre-generated HTML pages and their hosting services, ready-made e-mails for well-known institutions. Exploits, mailing lists and software for their collection, malware that can be used as a malicious email payload are offered.

In addition, it is common practice to use pre-compromised accounts to increase the trust of recipients and facilitate verification by technical means. For example, the sending of phishing emails by the UAC-0010 group was recorded by CERT-UA on November 7, 2022 using the @mail.gov.ua service [10].

All this makes it easier for criminals to operate and places new demands on the preparedness and vigilance of employees who work with electronic correspondence.

### **1.2.2. Malware statistics for phishing letters**

When investigating the problem of phishing, it should be noted that attackers actively use existing exploits and malicious software.

In Fig. 3 and 4 we show the statistics collected within the framework of this study for

one of the Ukrainian institutions of the financial sector. Fig. 3 illustrates the situation in 2021, and Fig. 4 - for the period from January to August 2022.

The average number of emails that contained malicious attachments by hour of the day for 2022 shows a significant increase in attacks compared to 2021. In both figures, we observe a peculiar peak in the number of emails with malicious attachments at 12 and 1 p.m., which, presumably, can be due to the fact that before the lunch break, the attention of employees is distracted, there is a subconscious desire to deal with correspondence faster, which can lead to inattention and mistakes - so social engineers may use this fact.

If you add up all the letters that come to the addresses during non-working hours, it will turn out that the peak of received correspondence actually occurs at the beginning of the working day. This requires the employee to be especially alert at this time.

Also according to Fig. 3 and 4, we can get an idea of the threat landscape (and the corresponding malware), which was actively used during 2021 and 2022. We see that a PDF-based attacks are being used, as well as targeting vulnerabilities in standard office applications.

According to 2021 data, significantly fewer letters were received during non-working hours than during working hours. In 2022, the difference between working hours and non-working hours is almost imperceptible. This fact can be connected with the intensification of the general background of attacks on Ukrainian institutions in the conditions of war, when the threats have become massive, 24/7, and are carried out by enemy cyber groups. Also Phishing-As-a-Service is used more actively.

## **2. Countermeasures and means of prevention**

### **2.1. Countermeasures**

Among the countermeasures and prevention measures, the following can be suggested:

- Analysis of how the organization looks from the outside (OSINT), for example with Maltego, theHarvester. That will allow you to identify e-mail addresses that have already been published on the Internet; preliminary statistics of mail systems (recipients of viruses and spam), which, in combination with the previous point, will

make it possible to determine VAP (Very Attacked Person) (Fig. 3, 4). Figures 3 and 4 show the number of phishing emails to different addresses in different colors. Thus, it is possible to single out those persons whose addresses are attacked more often, in order to take appropriate measures, and to pay more attention to them in the process of Security Awareness. Also, such graphs provide an understanding of linking attacks to reporting dates, important rallies, new exploits publication dates or other events.

- Control of appearance of phishing domain names (for example, with the DNStwist utility), will allow you to detect a targeted phishing attack at the preparation stage;

- Introduction of well-configured Secure email gateway;

- Sender Policy Framework (SPF);

- DomainKeys Identified Mail (DKIM);

- Domain-based Message Authentication, Reporting and Conformance (DMARC);

- stop words;

- investment control;

- geo-ip;

- sandbox.

- Support for updating all systems interacting with letters in an up-to-date state.

- Keeping Security Email Gateway, mail server and user endpoints up-to-date.

- Staff training and awareness raising, for example, as shown in [12, 13]. Staff training is a mandatory part of protection against phishing, as in fact the user becomes the "last line of defense" in case of possible malfunctions of technical means during targeted attacks.

- Means of personnel training on the basis of "false alarms". When organizing such events, you need to have a database of letters that will simulate the action of a phisher, in order to see if the user can recognize the danger and react adequately. In conditions of busy security departments, a convenient solution is automated means of generating various phishing letters [12].

### **2.2. Means of prevention**

In order to generate the required number of messages that allow training in large institutions, it is necessary to automate the process of creating the appropriate messages. Work on the development of natural language message generators for analytical languages has already been carried out, in particular in [14, 15].

Research on issues of generating messages of a given direction in synthetic languages, in particular Ukrainian, was carried out in work [15]. However, at that time, the means of generating texts in natural language had not yet

the other hand, at the time of writing, have the best performance both in text generation tasks and in other NLP tasks.

GPT-2, XLNet, and BERT were selected as specific neural networks on the basis of which the generator was written. They were neural networks that performed best in NLP tasks at the time.

With this in mind, this paper proposes an improved solution based on a model that works using the Happy-Transformer library and the GPT Neo 2.7B model in the Google Collaboratory Pro cloud service.

To generate a phishing message, the user enters up to 5 keywords, which allows you to adjust the direction of the generated message. Text is generated based on the model and templates. Templates are set in advance in order to teach the network to respond to the given topic of the letter. As part of the study, a set of typical templates was proposed (see Fig. 7 for an example).

The text is translated into Ukrainian using the Microsoft API in order to automatically achieve the orthographic adequacy inherent in synthetic languages. Next, you can insert the necessary references into the text, adjust the greeting and ending for the target example.

Corresponding messages can also be used to configure mail filtering tools.

Examples of generator operation are shown in Fig. 8-9. Further, messages can be sent, for example, to company employees to identify individuals most susceptible to phishing attacks. Then, with such employees, it is possible to conduct additional trainings on increasing vigilance and awareness in the field of social engineering attacks.

## Conclusions

Observations show that phishing against Ukrainian enterprises and organisations is currently a massive phenomenon, which is very dangerous. Many reasons have contributed to the increase in phishing activity. In particular, the need for technical resources to carry out phishing attacks can be easily achieved due to the automation of some technical functions, the openness of exploits, and the availability of malware samples, which makes it easier for low-qualified phishers to carry out attacks (Phishing-As-a-Service). During the war, cyber groups of the aggressor country and its satellites are also

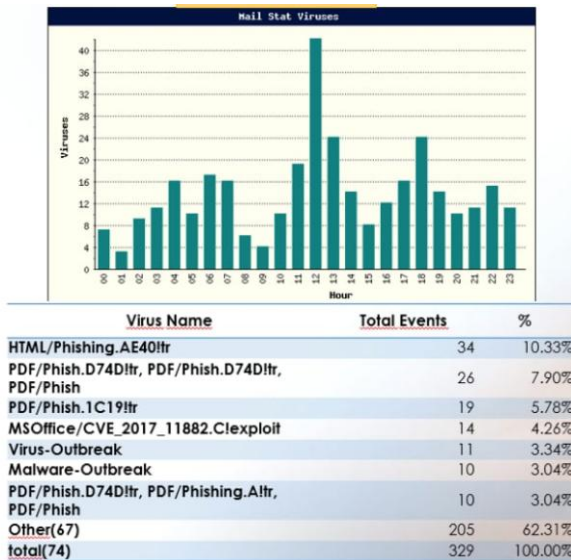


Figure 3: Average number of phishing emails by hours of day (2021)

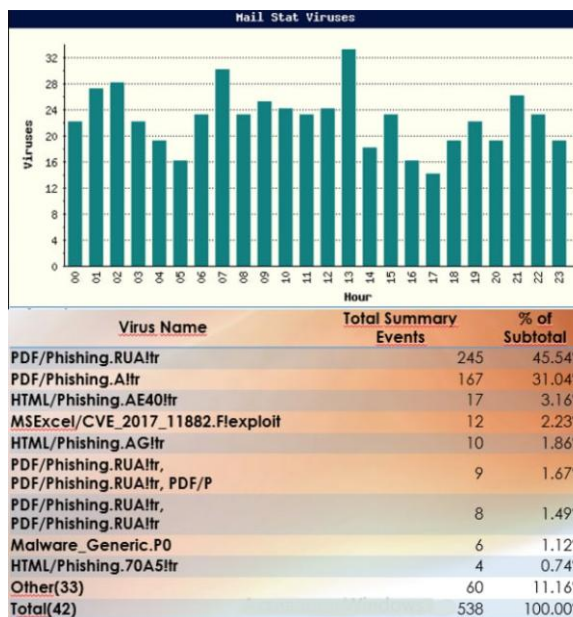


Figure 4: Average number of phishing emails by hours of day (Jan - Aug 2022)

reached the capabilities that they have at the present moment. In particular, in work [14] it is proposed to choose neural networks based on the Transformers architecture as the basis for the generator. The unsuccessful experiment of the authors showed that LSTM networks do not give the desired result for the tasks of text generation in Ukrainian language. Transformer networks, on

operate against Ukrainian enterprises and institutions.

During the research, features inherent in phishing attacks on Ukrainian enterprises and attacks lifecycles were analyzed. The main psychological factors that contribute to the success of attacks are anxiety, irritation and the desire to help; and an additional favorable factor is the fatigue of the workers. In these circumstances, it is important to offload staff who handle large volumes of correspondence, allowing them to systematically and diligently process incoming mail, and to strengthen the quality of mail filters and other protections.

The main means and measures for combating and preventing phishing attacks are highlighted. Special attention should be paid to appropriate measures to increase staff awareness of social engineering techniques, as well as regular training and "false alarms", that will make it possible to reinforce theoretical knowledge with practical actions. In conditions of constant stress, it is necessary to give clear instructions to the staff on the course of action in case of receiving letters from unverified contributors, for example, opening attachments in a virtual environment or in the cloud.

To automate the drafting of targeted phishing texts that can be used during vigilance training of personnel of large enterprises, a software solution based on the GPT-Neo model, the Happy-Transformer library and templates for simulating phishing letters is proposed, which, together with the translation into Ukrainian by means Microsoft API, made it possible to receive texts with a high level of similarity to natural language on a given topic.

## References

- [1] Threat report 2022. State of the Phish. URL: <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>
- [2] G. Aaron and oth. Phishing Landscape 2022. An Annual Study of the Scope and Distribution of Phishing. URL: <https://interisle.net/PhishingLandscape2022.pdf>.
- [3] Phishing activity trends reports. URL: <https://apwg.org/trendsreports/>
- [4] Cyber Attacks in Times of Conflict. URL: <https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details>.
- [5] Kevin D. Mitnick and William L. Simon. The Art of Deception: Control- ling the Human Element of Security. John Wiley & Sons, Inc., New York, NY, USA, 2003.
- [6] Ira S. Winkler and Brian Dealy. Information Security Technology? ...Don't Rely on It. A Case Study in Social Engineering. In SSYM'95: Proceedings of the 5th conference on USENIX UNIX Security Symposium, Berkeley, CA, USA, 1995. USENIX Association.
- [7] Charles E. Lively. Psychological Based Social Engineering. SANS Institute, 2003.
- [8] Ema Utamia, Anggit Dwi Hartantob, Sumarni Adib, Irwan Oyongb, Suwanto Raharjo, Profiling analysis of DISC personality traits based on Twitter posts in Bahasa Indonesia <https://doi.org/10.1016/j.jksuci.2019.10.008>
- [9] Vlasenko A., Stopochkina I., Ilin M. Methods of counteraction of bypassing two-factor authentication using reverse proxy //Theoretical and Applied Cybersecurity Vol. 3 No. 1 (2021): Theoretical And Applied Cybersecurity.
- [10] Кібератака групи UAC-0010: розсилання електронних листів, начебто, від імені Держспецзв'язку (CERT-UA#5570). URL: <https://cert.gov.ua/article/2681855>
- [11] KnowBe4 Top-Clicked Phishing Email Subjects for Q2 2022. URL: <https://blog.knowbe4.com/top-clicked-phishing-emails-q2-2022-infographic>
- [12] Usecure: Your Complete Guide To Employee Phishing Scams. URL: [https://cdn2.hubspot.net/hubfs/2707865/Your%20Complete%20Guide%20To%20Employee%20Phishing%20Scams%20\(1\).pdf](https://cdn2.hubspot.net/hubfs/2707865/Your%20Complete%20Guide%20To%20Employee%20Phishing%20Scams%20(1).pdf)
- [13] Phishing Simulator. URL: <https://phishinsight.trendmicro.com/phishing/test>
- [14] Automated email Generation for Targeted Attacks using Natural Language Avisha Das, Rakesh Verma (2018). URL: [https://www.researchgate.net/publication/328230780\\_Automated\\_email\\_Generation\\_for\\_Targeted\\_Attacks\\_using\\_Natural\\_Language](https://www.researchgate.net/publication/328230780_Automated_email_Generation_for_Targeted_Attacks_using_Natural_Language)
- [15] С.В. Іванченко, І.В. Стъопочкіна. Методи автоматизованої генерації фішингових повідомлень для тестування на проникнення //Матеріали Всеукраїнської науково-практичної конференції “Теоретичні і прикладні проблеми фізики, математики та інформатики”, 12-13 травня 2020, - с.257-260. (Methods of automated generation of phishing messages for penetration testing . In Ukrainian).



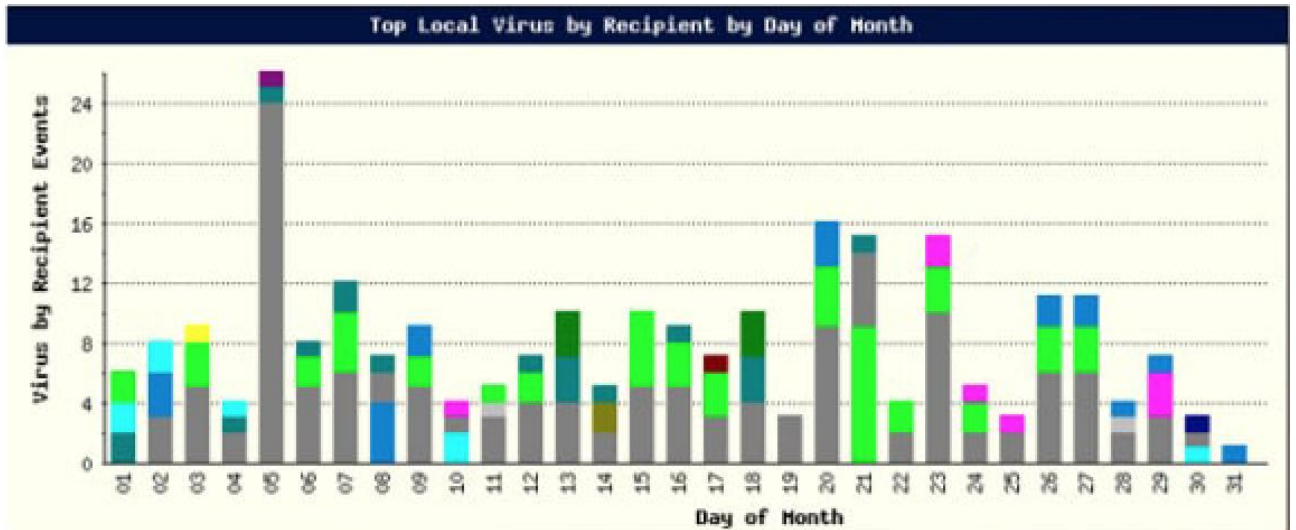


Figure 5: Statistics of received phishing emails by day of the month (average for 2021)

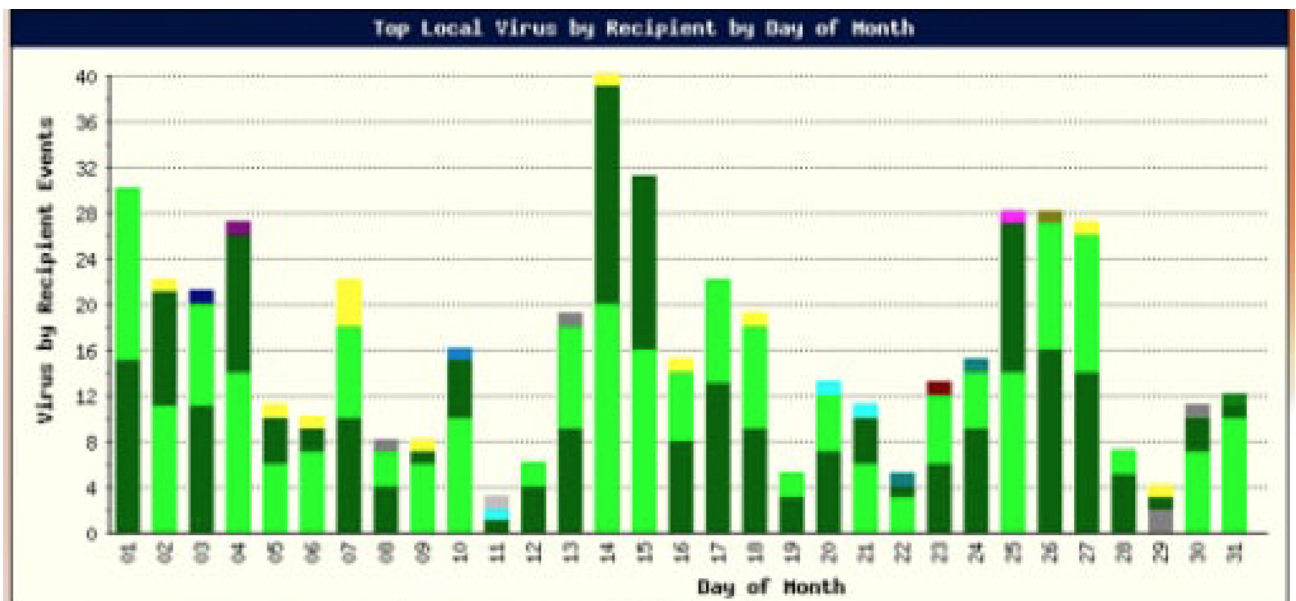


Figure 6: Statistics of received phishing emails by day of the month (average for Jan-Aug 2022 )

**Keywords:** <Keyword1>, <Keyword2>, ...<Keyword5>  
**Output:** <Greeting>, <Main text>, <Link>, <Finish words>

**Keywords:** support, present, exclusive, offer, anniversary  
**Output:** Hello,  
 On this cherished occasion, we'd like to present you with an exclusive anniversary offer. Please accept our most sincere thanks for your continued support [http://\\_\\_\\_\\_\\_](http://_____)  
 Enjoy!

Figure 7: Template example

Input  
Ukraine army email war link

Output  
Салют  
Мене звуть Олександр Шушкевич і я прослужив понад 33 роки в українській армії. Я також є дослідником електронної пошти та веб-сторінок і останні 4 роки проводжу дослідження клієнтів електронної пошти та проксі, тому я приєднався до Емського як співробітник 7 травня 2014 року. Мене завжди цікавило все, що пов'язано з електронною поштою, особливо її історія, і я хотів дослідити тему та спробувати написати про неї. Моєю метою було написати статтю, яка дає повне розуміння того, як працюють електронні листи та проксі та як вони використовуються людьми. Я був настільки звільнений, коли дізнався, що в Інтернеті немає статті на цю тему, і вирішив написати її. Це також єдина стаття, яку я коли-небудь писав, і я нею дуже пишаюся. Сподіваюся, вам буде цікаво, і, будь ласка, використовуйте його як натхнення для власного письма.  
Дякую за ваш час

a)

Input  
Ukraine army email war link

Output  
Hey,  
My name is Alexander Shushkevich and I have served for over 33 years in the Ukrainian Military. I am also an email and web researcher and have been doing research on e-mail clients and proxies for the last 4 years, which is why I joined Emsky as an employee on the 7th of May 2014. I have always been interested in everything related to email, especially its history, and wanted to investigate the subject and try to write about it. My goal was to write an article that gives a complete understanding of how e-mails and proxies work and how they are used by people. I was so exited when I found out that there is no article on this subject available on the internet and decided to write it.  
This is also the only article that I have ever written, and I am pretty proud of it. I hope you will find it interesting, and please use it as an inspiration for your own writing.  
Thank you for your time

b)

Figure 8: Email example 1: a) in Ukrainian b) the same in English

Input  
Microsoft email link customer help

Output  
Дякую  
Гарної роботи!  
Цей електронний лист було надіслано вам як пропозиція підтримки/запитання/інформації/річниця.  
Отримавши цей електронний лист, зверніться до адміністратора сервера. Ми надамо вам підтримку в найкоротші терміни.  
  
Щоб активувати підтримку, на яку ви заслуговуєте, натисніть на посилання, яке ви отримали як подяку за підтримку. Це займає лише одну секунду, і це варте вдячності, яку ви отримаєте. Я теж дочекаюся тебе внизу:  
  
<http://www.expect-support.net/>  
  
Дякую!  
  
І ось друга частина: подарунок ви отримаєте після закінчення терміну підтримки. Завдяки підтримці, яку ми запропонували за вашу допомогу, ви зможете отримати наступне:  
Це ексклюзивне повідомлення від Microsoft:  
Ви попросили отримати останню версію Outlook для свого облікового запису Microsoft з безкоштовною підтримкою. Тепер прийшов час його отримати.  
За нашу поточну підтримку

a)

Input  
Microsoft email link customer help

Output  
Thank you,  
Good work!  
This email has been sent to you as a support/question/info/anniversary offer.  
After you've received this email, please contact your server administrator. We will provide you with the support as soon as possible.  
  
To activate the support you deserve, click on the link you received as a thank-you for your support. It only takes one second, and that's worth the gratitude you'll have. I'll also wait for you at the bottom:  
  
<http://www.expect-support.net/>  
  
Thanks!  
  
And here comes the second part: the gift you will get after the support expires. Thanks to the support we have offered for your help, you'll be able to receive the following:  
This is an exclusive message from Microsoft:  
You have asked to get the latest version of Outlook for your Microsoft account with free support. Now it's time to get it.  
For our current support

b)

Figure 9: Email example 2: a) in Ukrainian b) the same in English