This publication examines fake news and the closely related phenomena of information security, namely cyber in/security. Phenomena such as *clickbait* (and the models on which it functions) and *malware* are considered, as well as their reversing interactions, known recently as "*phishing*." Signs by which these negative phenomena can be recognized are indicated, effective steps for proactive behaviour to neutralize them are likewise suggested.

**Key words:** fake news, disinformation, information security, cyber in/security, antivirus and antispyware software, clickbait, malware, phishing, models, proactive behaviour.

Fake news is one of the most topical themes of the present day. We rarely listen or watch a newscast that does not focus its "arrows" on this phenomenon, having been based on disinformation and propaganda for centuries, and which has peaked in 2017 [1] when it reaches the incredible growth of 365% over the previous year. – A fact that has its basis: 2016 was the year of the presidential race in America, a race that occurred under the sign of propaganda in a particularly large size and was
unscrupulous by its nature and which was mainly applied by the current President Donald Trump. False news is associated most often, but not primarily with political propaganda; it is the basis of asymmetric threats and hybrid wars, terrorism, natural disasters, science, urban legends, advertising, finance, etc. It is hardly possible to list all the various discourses without omission.

Fake news usually accompanies information security\(^1\) issues; to be more accurate – information in/security ones: clickbait, malware, phishing, social engineering, botnet, darknet. This publication addresses the first three of them; the others are subject to further research.

A clickbait is a special way of creating a title that allows distortion of the meaning of the text in order to draw reader’s attention: make them click on the promising start of the news. Clickbait headlines hold back the essence of the information cause, stirring up curiosity. Such vagueness, incompleteness is used as a bait, which is the essence of this complex word. The data of the etymological dictionary reveal the semantics of the word. The Oxford Dictionary gives the following definition of this construct: "(on the Internet) content whose main purpose is to attract attention and encourage visitors to click on a link to a particular web page."[2] The English etymological online glossary dates it back to 2011 and defines it as "internet content meant primarily to lure a viewer to click on it" – derived from "click" and "bait". The etymology of "bait" is revealed in the same dictionary as "food put on a hook or trap to attract prey" (1300), derived back from the old Norwegian beita "food, bait" especially for fish, from the another meaning of beita "cause to bite". The noun is related to the Old Norse word beit (pasture, pasturage) and the Old English bat (food). Figurative sense "means of enticement" is from c. 1400. [3]

This phenomenon arose from the fact that advertisers pay sites for the number of clicks, that is, transitions to the page where the banner is placed.

What are the models a clickbait is created on?

- Using an imperative mood, urging to immediately click on the banner and find out what the intriguing news is;
- The very news and its headline, in which, according to the “rules” of clickbait, there must necessarily be incompleteness, sometimes – on the verge of disinformation;

---

\(^1\) Cybersecurity and Information Security are generally used as synonyms in security terminology though there is certain difference between the terms. Shortly, Information security is all about protecting the information, which generally focuses on the confidentiality, integrity, availability (CIA) of the information. While cybersecurity is about securing things that are vulnerable through ICT (Information and Communications Technologies). It also considers the matter where data is stored and technologies used to secure the data. Part of cybersecurity about the protection of information and communications technologies – i.e. hardware and software, is known as ICT security.
➢ The immediate closeness to other provocative news creates an atmosphere of a blitz match, where the most biting and catching wording wins;
➢ Usage of many epithets, hyperboles, idioms and demonstrative pronouns. The first two means attract reader’s attention. The last two ones create a sense of trust between the reader and the site;
➢ Irrelevant and strange usage of too many exclamation marks, question-marks and three dots which aims at reader’s affect and the final goal – their click.
➢ Third-person singular appeals (It concerns the Bulgarian and Russian languages, for example, but does not concern the English language, where there is no special form of "you" for expressing courtesy and where the forms of the second person singulairia tantum and the second person pluralia tantum are the same). On sites where many people use clickbait, readers usually do not turn to "you" for expressing courtesy in the mentioned languages. An unconstrained, friendly "you" in such cases creates an atmosphere of a friendly conversation, as in the case of using demonstrative pronouns and idioms (noted above).
➢ Contradiction between an ordinary and extravagant, provocative title. Very often a clickbait header consists of two sentences. Usually the first of them describes an ordinary situation, and the second one hints at an unexpected turn of events and “fires” reader’s curiosity and imagination.
➢ One of the ”traps” of clickbait is a picture that contrasts with the title and thus allures the reader to click on it in order to understand “what is wrong”.

Information security experts' attention has been attracted by fake news because it is the root of malware distribution as well – malicious software. Malware is used as a collective term for various types of software designed to damage, disrupt, steal, destroy, or generally to perform negative and illegitimate actions within computer systems. Scott Nelson, SecureSet’s vice president, says fake news is the newest division in social engineering (social engineering attacks are the practice of obtaining confidential information by applying manipulation techniques to legitimate users, with the most commonly used email and telephone) and hacking. "Today, over 90% of threats rely on social engineering methods rather than on system vulnerabilities. <...> Over 99% of malware codes rely on the user to open an infected attachment or click on a link of a crafty forged webpage. In 2016, there is a 150% increase in social phishing, 600% more are the attacks with cryptoviral viruses, and over 40% of malicious codes today are viruses "gaining" directly from the ransom paid by inattentive users. "[4].

Recently, some phenomena all too often are observed: they interweave craftily with the wiles of clickbait and malware. These phenomena are of major importance to the individual / corporate
information security because they may become the reason a large amount of money to be stolen from their bank accounts. Over the past two months, the author of this study has noticed an unusual number of breakthroughs in the information security of her personal email, as well as in her friends and colleagues’ email (who shared their concerns about the matter), regarding their contacts with the relevant servicing banks of theirs. It is obviously about clients’ identity theft and an attempt to drain data from their profiles, and what is much worse - money from their accounts. In such cases hackers rely on the notice, grabbing customer’s attention while reporting about an expired account or expired bank account profile and requiring: "Confirm your identity", „Актуализирайте своя информационен персонал“ (literary "Update your information staff" which does not make any sense in both languages, it cannot be adequately translated because of lack of coordination between vocabulary and grammar in the subject of the email written in Bulgarian; reading such a message the customers might understand that they have to update their personal details).

One of the bogus bank email has a subject written in broken English which says “Servive your bank” (it is well known that there is not such a word in English like “serve”). It is written this way either to attract the readers’ attention to a word which meaning is not familiar to them hoping their curiosity to prevail: as to whether it is a matter concerning words with similar spelling like “serve”, “survive” or regarding something which is imminent to get acquainted with…within a click) or it is just the case when the message is written by an ignorant person. Here is another example of a bank notification (Fibank)

2. The message in Bulgarian: „Уважаеми клиенти, Известна информация за профила Ви липсва или е неправилна. <…> Моля, актуализирайте информацията си незабавно, за да можете да продължите да се радвате на всички предимства на профила си. че от време на време трябва да проверяваме информацията за профила, за да сме сигурни, че вашиите клиенти ще могат да използват нашите услуги правилно /изречението завършва без точка/ Искрено
Актуализиране на данните
Искрено ваш,,
PИБ"

It is pretty strange why the bank comments its clients like your clients.
dot/ Sincerely ... /the sentence is not completed/) After these lines an "Updating Data" banner follows. Finally, at the end of the email it is written: "Sincerely yours – TWO commas! They are followed by only the abbreviation of the bank but not by the Bank Director’s or the authorized employee’s name and their signature. We have already studied such a non-standard layout of a title and text featuring too many punctuation marks, inappropriate grammatical, syntactic, stylistic etc. lack of correspondence as one of the certain signs of fake news and other forgery which have to serve as prevention in order to be recognized and not to click on them. [5]

Such is the case with the subject of a mail (in English) sent by Netflix⁴ saying: “Notice you statut account was change” (three mistakes in this English sentence); the content of the message (it even seems strange that it is written correctly after such illiterate subject): “Dear Customer, your account was recently logged into from an unrecognized browser or device: Location: New Zealand, IP address: 2.47.255.255, Navigator: Chrome (Windows).” A banner in red follows after it which says “Update My Account”. And here the absent-minded, gullible or uninformed customer is to click on it (as it was supposed to in the above mentioned examples) and start entering the required personal data.

In cases as in preceding it is very important a person to rely on a modern and updated antivirus and antispyware software. If you are not sure it has helped, be alert in situations described in [5]. And if users still have doubts, before opening such files they must have proactive behavior: to contact their bank (or organization the file has been received by) and make an inquiry, to personally meet its representative at the bank/organisation office, and if advised, to follow the instructions given by the bank security officers. Such cooperation

➢ would help solve the problem;
➢ would provide additional information and knowledge about future behaviour in a similar situation;
➢ would provide timely clue to the information and cybersecurity department of the bank / organization for a probable breakthrough in the system;
➢ would facilitate more robust and efficient work of the cybersecurity staff of the respective bank / organization and their cooperation with the relevant departments of related companies to pool efforts to resolve such security breach issues (different banks have been subjected to such cyberattacks over the years as well as the National Revenue Agency in Bulgaria over the last years, even the computer systems in the country on the day of 2015 elections were subjected to cyberattacks, etc.).

---

⁴ Netflix is one of the world’s leading subscription service for watching TV episodes and movies on your phone with over 117 million members in over 190 countries.
The effect brought about by the implementation of the outlined steps would be very likely to yield good results from such cooperation, as in the case of the mail received by the bogus Fibank (not the genuine Fibank). The first steps to increase the bank cybersecurity apparently had already been made when two weeks after the commented mail of the bogus Fibank a new mail was received from it, but at the beginning, above the email subject, a bright red banner appeared, warning: "The letter you have opened contains links to a phishing site. We recommend that you do not open these links." If there weren’t such a warning, the subject of that mail would put the customer's attention off their guard just because the subject of the mail says it is needed some actions in relation to: "REQUIRED ACTIONS - Cash Memo [# 1265-3599] /30.03.2018“ to be taken.

In all these cases mentioned above, it is obviously the so-called „phishing“ or in other words – an attempt to drain the customers’ bank accounts and/or an attempted theft of users’ personal data. The word "phishing" is of English origin and is created as conscious distortion of the word fishing (“the sport or job of catching fish”, [2]), so we are dealing here with the common network fraud. Particularly those clever masters of “ice fishing” create addresses that at first cursory glance cannot be distinguished from the genuine ones. It is a type of Internet fraud, the purpose of which is to gain access to confidential customers’ data – logins and passwords or simply to infect their computer with malicious code. Phishing attacks are usually done remotely. The universal tool for phishing attacks is email. The goal of such attacks is to reach as many people as possible, as this increases the amount of the stolen personal data. Thus the attack is achieved by mass sending emails that have to convince the addressee to do one of the following:

➢ to open a link;
➢ to enter their password on a non-genuine, bogus website (for example, a copy of Facebook);
➢ to open a document attached to the letter;
➢ to install software.

A good example of such creativity can be considered the well-known site Yanclex.ru, whose owner was deprived of the domain by the court (the bogus site had a very similar spelling to the spelling of the genuine Russian site Yandex.ru). In Bulgaria, one of the most recent examples of such a phishing attack is a fake message from the National Revenue Agency, claiming the addressees owe taxes, and they have to pay them if they do not want to be fined. For more information, the authors of the mail had helpfully attached a document, containing the new legislation governing those fines. However, the document turned out to be nothing else than a virus, and the message was sent for the sole purpose of opening the document and installing that virus on the addressee’s computer.
Fake news and phenomena accompanying cyber in/security are a product of our time; they are like communicating vessels. From physics, it is well-known that communicating vessels is a name given to a set of containers containing a homogeneous fluid: when the liquid settles, it balances out to the same level in all of the containers. This physical law has its conformity to the phenomena studied in the present research. The difference lies in the fact that the interaction between the communicating vessels complies with proven physical laws and is therefore predictable, and the interaction between fake news and the accompanying phenomena related to cyber in/security, albeit being invariable, is unbalanced and unpredictable. Undisputed, however, is the relationship between fake news and cyber in/security: provided that there are phenomena such as clickbait, malware, phishing and similar to them, they are all a sure sign that it is a matter of fake news as well.

References:


Ilieva Diana Ivanova, PhD
University of Library Studies and Information Technologies, Sofia, Bulgaria
д-р Илиева Диана Иванова
Университет по библиотекознание и информационни технологии, София, България
Contact information:
Bulgaria, Sofia 1750
h. complex “Poligona”, block 13, entr. 1, floor 1, ap. 2
tel.: +359 878 131100; email: diana_edubg@abv.bg