

LINGUISTIC PECULIARITIES OF FRAUD IN DIGITAL MESSAGES AND PHONE CALLS

Since early childhood we start learning other people's body language and intonation. It helps us to understand if the speaker is telling the truth or lying. This knowledge also helps us not to become a victim of scammers and fraudsters, to avoid their attempts to manipulate our behaviour. But this threat is much more dangerous on the Internet, where a range of virtual scams have been significantly increasing. There's no body language or intonation in e-mail or social networks, generally we have only a text at our disposal. It means we must find some new approaches in evaluating possible threats.

As this problem has an international character and is also vital nowadays for our country, we decided to make a linguistic analysis of scams in the English and Russian languages.

Our research focuses on some typical examples and explains how you can protect yourself. It is especially important for those who are new on the Internet. Cybercriminals and scammers are unlikely to reinvent the wheel, so possessing some skills for scam identification you can provide your security in the future.

If you're new on the Internet, probably one of the first things you're going to do is set up an email account. Unfortunately, you can get lots of unwanted messages, which offer you a cheap credit and a wide range of different products and services. The best thing to do is delete the messages without reading, and then they won't damage your computer. Cybercriminals are smart psychologists: they become especially active before such holidays as Christmas, Easter, and of course Valentine's Day. So, if you receive an email on Valentine's Day with the words '*I love you*', you would definitely like to open it.

Probably one of the best-known scams is phishing. You receive an email which asks you to attend a site (the link is given in the email) and enter some personal information – this might be a password, a bank account number etc. The email might look as though it's come from your bank or some payment system. This can make you panic, open the email, click the link, and log in your account. Even if the message is rather convincing you must understand, it's a fake. If you click on the link and enter the information requested, cybercriminals can get your information and use it for their own aims. Phishing emails are an international

phenomenon: a basic text can be translated into different languages, and an email is then designed to imitate a well-known bank. On the other hand, they often contain spelling and grammar mistakes. Besides such emails often start with '*Dear customer*' rather than using your actual name. And finally, legitimate banks never request PIN numbers, or some other important information. Phishing emails of this type often threaten to close your account, because it's not been used for some time. To retain your account, the message says, you should log in; and of course, there's a handy link provided in the email.

If you possess any business you can also be followed by scams who try to issue fake bills for unwanted advertisements, products or services. You can receive a bill for a listing in some well-known business company. Scammers try to make you sign up the offer, but it has a hidden subscription trick. Scammers can also call your company pretending that a service or product has already been ordered and ask for a payment over the phone.

Technical support scams are very common nowadays. Scammers use different various techniques to make a potential victim pay for unnecessary technical support services.

These tech experts persuade you that they know everything about your computer, inform you how it got hacked by cybercriminals and many other details, so they easily gain your trust and immediately offer their help in solving urgent problems.

Furthermore, so-called tech scammers could persuade the potential victim to give them remote access to the system. They inform the victim, that additional software are required to be installed. So victims need to pay for this help, sometimes providing credit card details. In order to avoid getting scammed "by tech support specialists" we must follow some basic rules:

- don't trust phone calls coming from pretending tech experts, especially if they are requesting for personal or financial information;
- don't provide personal data to anybody, who suggests to solve your tech problem;
- don't allow strangers to remotely access your computer and potentially install malicious software;
- make sure you download software services only from official vendor sites;

Though secret shopper scams are very diverse, they have a common aim - stealing your money or your information. They promise you a large income. They announce that you can easily make up a lot of money doing what you love: shopping! It sounds too good to be true.

Job scams make proposals to work at home or invest in a business company. Scammers promise a job, high salary or large investment return following initial payments. They say that these payments may be used for getting uniforms, software, a business plan, a training course, paying taxes or fees. They are often promoted through spam e-mail or advertisements.

The victim is invited to click on a link to apply for the job. Then she is asked for social security number, the date of birth, the name of the bank and account number where they will want to deposit their pay check.

The use of a language or, more precisely, its misuse can also be an important characteristic of a scam. Grammar mistakes are easily found. It may be incorrect use of singular or plural forms '*my Lawyer will make preparation for my family to come over to your country*', mistakes in word formation '*I wait your urgent respond immediately*', incorrect prepositions as in '*and he died, since 1993*' and articles, use of capital letters etc. Still majority of these letters senders try to sound educated in different spheres of life. '*Good news dear, It is my pleasure to inform you that the latest development regarding the news from the New president of the United State of America to release all your fund through bank of america without any further delay.*'

Here we come across grammar mistakes, incorrect use of capital letters. Besides, '*United State*' is used in the singular. We don't see the person's name. A common beginning is something like '*Dear account-holder*'. Scammers don't worry about their poor use of English. Sometimes they even apologize for it, showing they are poor and desperately need help. But if you get an official letter, which promises you a good salary, which will be paid '*twice*' a month, referring to the '*issuing*' bank and strongly '*advice*' you to change your password, it is a phishing message. Of course, not every person has a perfect grammar and spelling, but there are some signs, which prove that this message or website could be a scam. They often use an old-fashioned language: '*We are assigned to render advice and assistance in line with your winning claim process*'. In order to pass spam filters, they use foreign languages. Words are often written in capital letters. Even in everyday usage, all capitals are considered to be rude. But in business letters, if all the message is written in ALL CAPITAL LETTERS, the chances of a buyer to have a problem with the purchase strongly increase. Incomplete or rambling sentences just don't make any sense.

During our research we analyzed Russian and English scam messages and found out that all scams usually consist of three parts: a greeting, a body and a closing.

English scam messages (18.9 %) usually start with typical **greetings** like '*dear*', '*dear sir*' '*dear friend*' '*dear madam*', Russian messages also often begin with the word '*дорогой*' (11.9 %). They also start with words '*Здравствуйте*'

'*Добрый день*' '*Доброго здоровья*', '*Приветствую*', '*Уважаемый*'. Still we found out that a great number of Russian messages (45.2%) don't have any greeting. They can start with words '*Вы хотите...*', '*Я адвокат*', '*Ваш caйм*'. In English messages we didn't find such examples. Both Russian and English messages approximately contain the same number of greetings, which start with the word '*Attention*', (Russian-9.5%, English-10.8 %). The same can be said about the greeting '*Good day*' (Russian-19 %, English-21.6%). The analysis showed some similarity in the **body** of the message. Scammers often send proposals to make a purchase (11,3 % in Russian, 11,8% in English) or propose a kind of award. Analyzing typical features of **conclusions** we found out that such words as '*best regards*' or '*regards*' are almost twice as much used in Russian (10.3 %) than in English messages (5,7 %). On the contrary '*sincerely yours*', '*yours*' dominates in English ones (11.4 %, 8.5 %)). We didn't find any request for response '*look forward, hear from you, I am waiting to hear from you soon*' in

Russian e-mail, in English-8.5 %. A common feature of Russian and English messages is that sometimes (in Russian-24.2 %, in English-17.1%) such letters don't have any closing at all. Scammers pretend to represent famous companies and organizations, including the police, banks or utility companies. Telephone interactions are not often considered to be a kind of cybersecurity, yet they play a crucial role. We tried to gather information and analyze publicly available IRS phone scam recordings, posted on YouTube. Such recordings are not ideal as they are made by people who know that such calls are scams and don't participate in the conversation just as an unsuspecting target. Still these calls tend to take similar forms, they may be a subject for linguistic analysis. Phone scams follow a rigid structure in which calls pass quickly to a proof phase that convinces the target in the necessity of their service and then comes a sales phase.

Really words have an immense power. The language of scams is as powerful and captivating to some people as a great literary work is to someone else. We should realize that behind that official professional sweet-sounding language there may be a wolf in sheep's clothing. Still many people become victims of telephone fraudsters.

We made a survey and found out that only 7 % of pupils could trust those sounding like a nice person. But if the speaker - sounds competent and seems to know what he is talking about already 28 % are ready to trust him. The trick offering to help with a problem can also be effective, so 10 % of our pupils are ready to accept such help. On the other hand, our pupils seem rather cautious, when they are informed about some unexpected award, none of them was ready to get such proposal. Though 56 % of my peers claim they - can easily determine a fraudster, the results of the survey show they are still rather vulnerable, as 21 % admit having had a negative experience of being fooled. 28% of the pupils honestly admit that have difficulties in identifying a fraudster Scammers often use these tricks for identification. If you receive a scam call, write down the number so that police can identify scammers and take appropriate actions:

- never send money, or give credit card information or online account details to someone you don't know who contacts you by email and asks for money;
- delete Spam e-mails, don't waste your time even opening them;
- be extremely wary of any job, loan, investment or any other offer that requires you to pay upfront fees;
- don't give personal or financial information in response to emails that look like they're coming from your bank or any other financial institution;
- be careful of the language you read on websites and in e-mails sent to you, don't trust anybody;
- keep in mind that attackers may also use scare tactics to lure you into revealing personally identifiable information;
- don't be in a hurry as a serious company will always wait, don't panic and don't make a decision you'll regret. And you should also follow your intuition.

Words play a vital part in any society. We use them to communicate ideas, feelings and knowledge and to understand the intentions of others, but they can also be used for evil. People must know about the language features of phone and

email scams which will help them protect themselves against any information attack. Even though computer users are getting smarter, and the antifishing tools they use are more accurate than ever, scammers are still succeeding. Using promises or threats of financial or physical danger they make people lose thousands of dollars. Paying attention to grammar, spelling and key phrases can be helpful in the identification of the scam language.

While many people claim they are not going to trust anybody on the phone or in social networks, fraudsters are well prepared for our skepticism and constantly invent new effective tricks, new fraudulent e-mail schemes to make people believe them. They still succeed as they promise a quick and easy rewarding and know very well what strings might be attached.

I hope that my research and my booklet will be useful for teenagers and adults, and they will learn not to trust anybody on the phone or in social networks. And I strongly believe, that if teenagers and children are aware of different types of scams and safe ways of using the net, they will be able to tell their elderly grandparents and relatives how to stay safe online.