Cybersecurity and related challenges in the context of the global pandemic

Zurab Gorgodze

Head of the Office of International Relations at the Thomas Jefferson Research Center

Poti 2020

Introduction

Cyber security, or IT security, refers to the security of technological devices such as computers and smartphones, as well as computer networks, both private and public, as well as the Internet. The cybersecurity sector is gaining momentum due to its dependence on computer systems in most societies. This applies to the protection of hardware, software, data, people, as well as the procedures by which systems are accessed. Computer security measures include the physical security of systems and the security of information stored on them.

In general, cybersecurity ranks first among the seven main directions in the concept of security, as inaction with the challenges it faces could do more harm than good to the state's conventional controversy.

The technological revolution and the increasing use of computer hardware have significantly increased the importance of cybersecurity, as a result of which states have developed cyber security strategies (Estonia was the first of the EU and NATO member states, 2007) and increased the budget to improve their infrastructure. However, in May 2016, the European Parliament for the first time published the General Data Protection Regulation (GDPR), which provides protection of personal information of citizens of EU countries.

In 2020, the announcement of COVID-19 as the global coronavirus virus, a global pandemic, has led to an increase in Internet usage and a new phase in technological development. Corona virus has introduced information technology in other ways. Companies, corporations, public and private institutions have switched to online work mode, which can be said to have created quite a solid ground for this trend in the future. In contrast to the transition to online work and Internet consumption, the challenges posed by cybercriminals have increased, and the Internet has never been as vulnerable as it is today.

The impact of the pandemic on digital behavior and cyber infrastructure

Today, everything has shifted to a very large dose of the Internet space, and the prediction of this in the past 2019 can be said, that it was impossible. Along with the use of the Internet, there are also threats to government communications, including the work of online video conferencing organizations of international organizations. This has become particularly attractive to special services and hackers. The dangers of disseminating information that may relate to state secrets and similar sensitive topics have increased. Schools and universities have also switched to online work, which has led to the creation of various applications and an increase in their consumption. Notably, schools in New York have blocked the use of Zoom because the research has shown that its use could end up stealing users' personal information.

Due to the fact that consumers are switching to online mode, the number of e-commerce and e-commerce transactions has also increased, which poses a particular threat to both consumers and large and small, private or public institutions.

The spread of the disease has had a huge impact on the digital behavior of Internet users not only in the affected areas, but around the world. Globally, authorities such as the World Health Organization (WHO) and the National Health Commission of China (NHC) use digital systems to send and receive information about the nature and extent of infections to inform the public how to prevent the virus. Also what to do with it, In the event of infection. It should also be noted that the Chinese government has published a mobile app that monitors people and provides them with information about whether they were in close contact with a person infected with coronavirus.

A similar trend was noticeable in Georgia when an application called "Stop Covid" appeared on various mobile phone application systems, which was downloaded by about 150,000 users in about 24 hours after its release. The app does not require registration, but requires permission from the microphone and location, which has made a lot of people think about whether to use this app because they have doubts about its security. There is a theoretical

risk, that the app may be updated and new features may be added, which may increase user access to more information through the app.

Cybersecurity is mainly focused on unauthorized change or avoidance of user data, as cyberbullying threatens the confidentiality of digital information. The word coronavirus is probably one of the most searched words in the entire internet space today, and the reason is obvious. Search engine, this is a program that helps us find data faster on the Internet or on the website, using text keywords. Internet search engines are currently overloaded with various keywords, from which the following keywords are mainly identified: corona, virus, coronavirus, COVID-19, China, Wuhan disease, and other keywords related to the pandemic. The proliferation of information about the spread of coronavirus and their search has significantly shifted the Internet, increasing the possibility of using malicious code for cybercriminals, which at the same time disguises information about coronavirus and distorts its authenticity.

The art of collecting sensitive and confidential information of a person using his own weaknesses is known in cyberspace as a social engineering. Social engineering is a psychological exploitation used by cyber scammers(individuals who obtain various confidential information through cyber-attacks) to skillfully manipulate people and carry out emotional attacks on innocent people. Social engineering methods also use psychological tricks to create deception. Social Engineering This is a psychological manipulation and attack in which an outsider conducts a user interrogation through deception in order to gain monopoly on the system or network and uses e-mail, phone call, personal correspondence or psychological observation of a person too. In this way, it receives authorized user data and is able to access the system or network based on them. Cybercriminals are making good use of social engineering to attack vulnerable victims, obtain confidential information, and carry out other attacks using such information. In the case of Coronavirus, cybercriminals are now using the advanced form of phishing called Spear Phishing, which aims to obtain information from influential individuals or various corporate associations.

In order to obtain personal information, medical institutions have recently become the most vulnerable facilities. Protecting the computer system of private medical facilities is the responsibility of this facility itself. It is imperative to develop various recommendations for improving the cyber infrastructure of medical institutions and to create a safe working environment for them, especially when prescriptions, medications and various operations are performed electronically in medical institutions.

It is noteworthy that in the conditions of the pandemic, e-commerce and online stores have significantly increased, where payment is mainly made through electronic transactions. A lot of online store pages have been created on social media lately, which could be imitations of fake or cloned websites. Often, such sites are hosted by cybercriminals who may steal personal information, influence financial matters, or disrupt various digital transactions.

As mentioned above, in the context of the global pandemic, the trends of online stores and e-commerce have already increased and increased, thus increasing the field of interest of cybercriminals in this direction. Against the background of e-commerce, e-transactions are also on the rise, but their security is not as secure as in large corporations. Therefore, before making an online transaction, it is important to note that:

- Spelling and grammatical errors on websites. Inconsistent grammatical expressions are a sign of falsity.
- Observe contradictory statements and ambiguous instructions on the website.
- Follow the instructions for emergency treatment, especially in the case of a known critical case such as coronavirus.
- The website often contains ambiguous contact information, including unavailable phone numbers, incorrect e-mail addresses, physical or legal addresses, incorrect markings, and many other details whose images are suspicious and also contain signs of fraud.

By following the recommendations above, you will be able to avoid the possibility of your banking and financial information being stolen by cybercriminals. Do not provide your

banking information to suspicious websites unless you are confident in their authenticity, which can be verified by contacting customer service staff or communicating via email.

Disinformation in the context of the global pandemic

The spread of the new coronavirus and the restrictions imposed on the world's population, in the areas of personal freedom, economic activity and public life, have turned the lives of billions of people upside down. Powerful digital platforms have the ability to disseminate information very quickly, under the same conditions, cybercriminals can also develop information with false or misleading content in circulation, which poses an even greater threat to the well-being of the population. It is important to check the information as soon as possible, but unfortunately not everyone has the opportunity to do so.

The coronavirus crisis has led to an increase in global, online misinformation, cyber-espionage (espionage) and the disruption of operations. Which includes dozens of countries, but the most important are Russia and China. Amid a pandemic that has claimed tens of thousands of lives, various analysts have noted that hackers, in parallel with attempted attacks on international organizations (which are trying to react against Coronavirus), have seen a sharp increase in targeted misinformation campaigns on social media.

Sputnik News published an article on January 22 stating that the spread of Coronavirus was linked to NATO and that it was a weapon created by them. This was the first misinformation about the Corona virus to spread on social media. Also, the Arabic version of Sputnik published an article blaming American laboratories for creating the Corona virus. The purpose of this information was to create different attitudes about conspiracy theory in the target groups and to manipulate the masses against the Western World.

Russia has been successfully developing a propaganda machine and has been spreading misinformation in various countries for years, influencing certain social groups and manipulating them, which threatens the principles of democracy.

In addition to the Russian-Chinese duo, Iran is also involved in spreading misinformation about the global pandemic of SOVID-19. This may be a complex campaign aimed at reducing public confidence in Western countries. It is noteworthy that under the pandemic, all three states are spreading similar fake narratives.

Sputnik, in the style of faded Russian propaganda, wrote that the Pentagon-funded biological laboratories were involved in the creation of COVID-19 around the world. As expected, the Lugar Laboratory in Georgia was also found at the center of this frequently repeated conspiracy theory. The story has been widely circulated on Twitter, Facebook and other social media platforms.

In fact, Lugar's lab in Georgia is the mainstay of the COVID-19 pandemic. The lab was opened in 2011, with the help of the United States, to fight infectious diseases. Lugar's lab is a critically important facility for detecting and responding to potentially deadly viruses before they spread. The Georgian government has tried to invite Russian experts to visit the laboratory, but Moscow has refused to do so because it would interfere with the Kremlin's propaganda agenda.

In the modern technological world, misinformation is one of the most powerful tools that often generates conflicts within the state, threatening both local and national interests. Disinformation is a huge challenge for both human security and national security. The global pandemic and the global population's dependence on the Internet have made this challenge even more feasible, as it is in these conditions that groups of disinformation and cybercriminals are trying to become more active. Most of the misinformation is related to the corona virus. Some misinformation is related to the creation of the vaccine, with some different treatments against the coronavirus. For example, we can cite a person who drank hot water in order to think that he would understand one of the mechanisms of the fight

against the virus. The same can be said for information related to vodka treatment, which mainly serves to mislead the public consciousness.

Also interesting is the fact that some websites ask users to register to see this or that information related to the Corona virus, which is dangerous and pushes users to share their personal information. Therefore, Internet users should definitely follow cyber hygiene, as they do not become victims of cyberattacks, which may damage their financial or mental condition.

Conclusion

In conclusion, it can be said that due to the growing dependence of the Internet space on the global pandemic, the lifestyle of each individual has changed significantly and the nature of the actions of various institutions, organizations, companies and corporations. The global challenge, in the form of COVID-19, has created a public mood around the world that the world will no longer be the same as it was before the pandemic. Cybercriminals have been able to take advantage of this situation and, consequently, the level of cybercrime has increased compared to previous years. Based on the issues discussed in the paper, it is clear that companies, organizations and various public or private institutions in the post-pandemic reality will move to a completely new stage of action and will try to introduce new trends.

In order to prevent the spread of personal data, it is necessary for users to follow cyber hygiene in order to avoid problems caused by cyberattacks.

The global pandemic has become the best event for disinformers, which may pose a threat to individual, local and national security.

Bibliography

- B. Atkins and W. Huang, "A study of social engineering in online frauds," Open Journal of Social Sciences- 2013.
- Tackling the Cybersecurity impacts of the Coronavirus outbreak as a challenge to internet safety – Kenneth Okereafor – National Health Insurance Scheme. Olajide Adebola – The University of Edinburgh.
- COVID-19: Impact on the Cyber Security Threat Landscape – Francois Mouton – Noroff University College. Arno de Coning – North West University South Africa.
- https://e-estonia.com/estonia-as-an-international-cybersecurity-leader/
- https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/
- https://www.cnbc.com/2020/02/10/china-launches-coronavirus-app-to-detect-whether-users-have-come-in-close-contact-with-the-sick.html.
- https://pia.ge/ka/news/covid-19/stop-covid-aplikatsia-24-saatshi-150-000-ze-metma-pirma-gadmotsera/
- https://netgazeti.ge/news/444042/
- https://en.unesco.org/news/disinformation-silent-weapon-times-pandemic
- https://www.dw.com/en/disinformation-and-propaganda-during-the-coronavirus-pandemic/a-52970643
- https://euvsdisinfo.eu/disinformation-can-kill/
- https://www.gfsis.org/ge/blog/view/1067
- https://techcrunch.com/2020/04/05/zoom-new-york-city schools/?fbclid=IwAR1OePLOBSclQiibhOh6QfuWuseu4pk_Fv0QVKgh8-ee6rdutqoMpRbOaNs