Cybersecurity: information and defence against data phishing

Cristiana SÎRBU,
University of Agricultural Sciences and Veterinary Medicine Bucharest, Faculty of Land Improvement and Environmental Engineering, "Gheorghe Ionescu Șișești" Academy of Agricultural and Forestry Sciences, Soil Science, Land Improvement and Environmental Protection Section, The Ecological Initiative and Sustainable Development Group Foundation
cris_sirbu@yahoo.com

Abstract
The paper presents the knowledge and information gained from participating in various events and workshops dedicated to cyber security. This highlights the need for information ownership in order to protect oneself in the jungle of data phishing, in a world that is constantly changing and where digital technology is the main means of conducting business in a modern society. Threats are evolving day by day and are difficult to contain, and this has highlighted the need for cyber security and cyber defence regulations. In the current context of digitization and technology, cybersecurity is a priority for every state.

Keywords: technology, digitization, security, strategy.

1. Introduction
Almost everyone and everywhere is talking about cyber defence, but it is a huge amount of information and thousands of years of work by programming and programming teams.

Threats in this vast field are evolving every day. It's an unmanageable avalanche that can swallow up the data protection work of super-professional teams like a giant in a fairy tale in seconds.

Cyber-attacks and cybercrime are growing in number and sophistication across Europe. The future is uncertain, with the trend expected to continue to grow.

2. Results and discussions
A number of critical sectors such as transport, energy, healthcare and finance have become increasingly dependent on digital technologies to run their core businesses.

Digitalization offers enormous opportunities and provides solutions to many of the challenges facing Europe.

Data phishing is the most common method of theft. Data phishing is a technique whereby an attempt is made to obtain sensitive data, such as bank account numbers, through a fraudulent request by email or on a website, where the perpetrator poses as a legitimate business or trusted person. This method of obtaining information can seriously damage both financial and reputational damage to corporations, institutions, business, academia and the many sectors that use digital technology [1].

Cyberspace is characterized by the absence of borders, creating opportunities for the development of the knowledge-based information society and risks to its functioning.

The more computerized a society is, the more vulnerable it is, and ensuring the security of cyberspace must be a major concern for all actors especially at the institutional level, where the responsibility for developing the security and implementation of coherent policies [2].

Cyber security is the application of technologies, processes and controls to protect systems, networks, software, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against unauthorized exploitation of systems, networks and technologies.

The European Union Directive on cyber security measures, known as the NIS Directive2 (by Law No 362/2018) on ensuring a high common level of security of networks and information systems, in conjunction with the provisions of Article 72 of the Treaty on the Functioning of the European Union have become obvious national responsibility and require regulations in the field of cyber security and cyber defence.

The EU cyber security strategy aims to strengthen the Union's resilience to cyber threats and to ensure that all citizens can benefit from trusted digital services.

In October 2020, at the Extraordinary Meeting of the European Council, EU leaders called for strengthening the European Union's ability to: protect itself against cyber threats, ensure a secure communication environment and ensure access to data for law enforcement and judicial purposes.

On 22 March 2021, the Council adopted conclusions on the Cybersecurity Strategy, which underline that cyber security is essential for building a resilient, green and digital Europe [3].

As a dimension of national security, the issue of cyber security and defence has become a priority.

Romania's Cyber Security Strategy for the period 2022 - 2027 and the Action Plan for the implementation of Romania's Cyber Security Strategy for 2022 - 2027 must ensure complementarity with the provisions of the European Union but also with a number of domestic ordinances (e.g. Emergency Ordinance 104/2021 establishing the National Cyber Security Directorate and at the same time with measures on cyber defence with specific aspects manifested in cyberspace). So, we are on the right track.

Romania's National Recovery and Resilience Programme (NRRP) has taken on the implementation of the measure "Ensuring the cyber security of public and private entities that own critical infrastructures.

Cooperation between the relevant institutions and civil society, academia and the private sector is the basis for the development of effective cybersecurity partnerships and the legal and institutional framework for organizing and carrying out cybersecurity and freedom defence activities.

Public international law puts conceptual uncertainties and differences in interpretation under scrutiny, particularly with regard to attribution of malicious cyber activities.

Concepts, solutions from the international environment that are related to the realities and specificities of legislation and institutions in the field, the creation of networks and systems accompanied by the adoption and development of a regulatory and institutional framework strengthen confidence in our common cyber future, both in the European Union and in Romania.

By ensuring resilience through a proactive approach and deterrence, Romania becomes a relevant player in the international cyber security cooperation architecture.

3. Conclusions

As a result of actively participating in workshops and various events, I have learned some of the essentials of modern cybernetics:

- Collective intelligence, which is not all one with the IT-ist, is about perfecting systems where the citizen is not harassed, is informed and protected;
- Access to technical information must be restricted;
- Malicious' operators see it as a weapon and the cybersecurity system sees it as an art;
- Threats evolve daily.

Security is not the pinnacle of some companies it is the prerogative of us all.

Cybersecurity is considered an extremely important part of national security. There is therefore a need to develop a cyber security culture among users of information and communication systems, who are often insufficiently informed about potential risks and solutions to counter them [4].

Widespread knowledge of the risks and threats to which cyberspace activities are exposed and how to prevent and counter them requires effective communication and cooperation between the specific actors in this field.

Acknowledgements

The study was conducted by The "Ecological Initiative and Sustainable Development Group" Foundation with the main purpose to be a connection between institutions, academia and civil society in order to inform and facilitate the access to information.

References

[1] "Digital Innovation Summit Bucharest," 16-18 April 2024.

[2] *European Union Agency for Cybersecurity, Romanian Cybersecurity Strategy.*

[3] in *DigitALL 2023 Conference*, 2023.

[4] "ZF Cybersecurity Trends 2023: How many cyber defence solutions does a company need and who should "run" them?," 29 May 2023.