Romanian Association for
Information Security Assurance

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume VII
eISSN 2393-0837

CyberCon Romania
2020

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume VII

A scientific conference organized by the
Romanian Association for Information Security Assurance

CyberCon Romania
2020

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

The International Conference on Cybersecurity and Cybercrime (IC3) is an annual scientific conference, with the purpose to encourage the exchange of ideas about the evolution of cyberspace, information security challenges, and new facets of the phenomenon of cybercrime. The event provides the appropriate framework for students to present their research in this field.

The Proceedings of the International Conference on Cybersecurity and Cybercrime includes scientific papers reviewed by the *Editorial Board* that consists of experts from academic police structures and university departments, their work taking place under the guidance of the *Advisory Board*, composed of internationally recognized personalities from the academic field.

Proceedings of the International Conference on Cybersecurity and Cybercrime
Online ISSN: 2393-0837
Print ISSN: 2393-0772
DOI: 10.19107/CYBERCON
URL: https://proceedings.cybercon.ro

The International Conference on Cybersecurity and Cybercrime is part of the **CyberCon Romania** event, organized by the Romanian Association for Information Security Assurance.

CyberCon Romania brings together experts from public institutions, private companies, and universities, for raising the level of awareness and embodies the cybersecurity culture.

Website: www.cybercon.ro

The Romanian Association for Information Security Assurance (RAISA) is a professional, non-governmental, non-partisan political, nonprofit, and public benefit association.

Founded in 2012, the association started as an initiative with the aim of promoting and supporting information security activities in compliance with applicable laws and creating a community for the exchange of knowledge between the experts from the public, private, and academic environment. Its vision is to encourage the cybersecurity research and education, and to contribute to the creation and dissemination of knowledge and technology in this domain.

Website: www.raisa.org

CONFERENCE COMMITTEES

EDITORIAL COUNCIL CHAIRMAN

Professor **Ioan C. BACIVAROV**, PhD
University Politehnica of Bucharest, Romania
Faculty of Electronics, Telecommunications and Information Technology

INTERNATIONAL ADVISORY BOARD

Professor Emeritus **Alessandro BIROLINI**, PhD
ETH Zurich, Switzerland

Professor **Angelica BACIVAROV**, PhD
University Politehnica of Bucharest, Romania

Professor **Fabrice GUERIN**, PhD
ISTIA, University of Angers, France

Professor **Daniela-Elena POPESCU**, PhD
University of Oradea, Romania

Professor **Sandeep TIWARI**, PhD
Amity University, India

Professor **Ton van der WIELE**, PhD
Erasmus University Rotterdam, Netherlands

ORGANIZATION COMMITTEE

Ioan-Cosmin MIHAI, PhD
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania

Gabriel PETRICĂ, PhD
University Politehnica of Bucharest, Romania

Ionuț-Daniel BARBU
University Politehnica of Bucharest, Romania

TABLE OF CONTENTS

Cyber Attacks in Online Commerce **5**
Veronica Ana-Maria CHIOVEANU

Vulnerabilities of EU Large-Scale IT Systems Used in Law Enforcement Cross-Border Information Exchange **13**
Iulian-Marius COMAN, Aurelian-Gabriel BĂDIȚĂ, Marin-Claudiu ȚUPULAN

Security Services in IP Networks **19**
Marian-Ştefan GONCIULEA

Legal Aspects Regarding Cybercrime **27**
Virgil-Corneliu TUDOR

Types of Cyber Attacks **33**
Eduard-Alexandru NEDELCU

Using AI to Defense Against Cybercrime **39**
Andrei-Costin MIRON

Cybercrime Phenomenon in Europe and Romania **45**
Răzvan ZAMFIRACHE

An Analysis on Phishing Phenomenon **49**
Antonia-Ruxandra CONSTANTIN

Analysis of Computer Attacks **55**
Adrian-Cristian PLOIEȘTEANU

Research on Cybersecurity Education and Vulnerability Awareness in Educational Ecosystems **63**
Daniela IONAȘC, Sabina-Daniela AXINTE, Daniel BUCĂTARU

Cyber Attacks in Online Commerce

Veronica Ana-Maria CHIOVEANU
University Politehnica of Bucharest, Romania
vera.chioveanu27@gmail.com

Abstract

Security in online banking and e-Commerce applications is very important both at the administrative level and from the user perspective. The internet has played a key role in changing how we interact with other people and how we do business today. As a result of the internet, electronic commerce has emerged, allowing business to more effectively interact with their customers and other corporations inside and outside their industries. One industry that is using this new communication channel to reach its customers is the banking industry. The e-banking system addresses several emerging trends: customer's demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. The challenges that oppose electronic banking are concerns of security and privacy of information. This paper will first discuss about online banking transactions; secondly, it will talk about e-commerce concept. Thirdly, the security and privacy attacks of internet banking, and fourthly the security measures to fight against e-commerce attacks.

Keywords: transaction, security, online banking, e-commerce

References

[1]. Online Transactions and Security of e-Transactions. [Online]. Available https://www.toppr.com/guides/business-studies/emerging-modes-of-business/online-transactions-and-security-of-e-transactions/.
[2]. J.E. Jarrett, Internet Banking and E-commerce: A Consumer Perspective.
[3]. What is ecommerce? [Online]. Available: https://ecommerceguide.com/guides/what-is-ecommerce/.
[4]. P.O. Magutu, E-Commerce Products and Services in the Banking Industry: The Adoption and Usage in Commercial Banks in Kenya, IBIMA Publishing Journal of Electronic Banking Systems http://www.ibimapublishing.com/journals/JEBS/jebs.html.
[5]. V. Jolly, The Influence of Internet Banking on the Efficiency and Cost Savings for Banks' Customers, Int. J. Soc. Sc. Manage. Vol. 3, Issue-3: 163-170.
[6]. E. Gamblin, Online Payment Security: 5 Steps to Ensure Safe Transactions. [Online]. Available: https://www.business.org/finance/payment-processing/online-payment-security-5-steps-to-ensure-safe-transactions/.
[7]. J. Gualdoni, A. Kurtz, I. Myzyri M. Wheeler, S. Rizvi, Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050917318100.
[8]. Z. Omariba, Security and Privacy of Electronic Banking, IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012 ISSN (Online): 1694-0814.

Vulnerabilities of EU Large-Scale IT Systems Used in Law Enforcement Cross-Border Information Exchange

Iulian-Marius COMAN
European Agency for Law Enforcement Training
iulian.coman@cepol.europa.eu

Aurelian-Gabriel BĂDIȚĂ
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
gabriel.badita@academiadepolitie.ro

Marin-Claudiu ȚUPULAN
Ministry of Internal Affairs, Romania
claudiu.tupulan@mai.gov.ro

Abstract

A borderless Europe needs to ensure continuous and secure exchange of data and information between the law enforcement authorities. This needs to be done through monitoring technology development and identifying large-scale IT systems protection from emerging threats. Decision making is never based solely on knowledge of technical issues, as the potential and expected benefits of implementing a particular technology depend specifically on the architecture of system data and information. Cybersecurity attacks on these systems can be explained starting with the attackers and targets, the approach to compromised system and the route used to break into the system.

Keywords: large-scale IT systems, law enforcement cooperation, intelligence-led policing, information exchange, smart borders, cyberattacks

References

[1]. Baldaccini, Anneliese, "Counter-Terrorism and the EU Strategy for Border Security:Framing Suspects with Biometric Documents and Databases", European Journal of Migration and Law, 10(1), 2008.

[2]. Besters, Michiel and Brom, Frans W.A., "'Greedy' Information Technology: The Digitalization of the European Migration Policy", European Journal of Migration and Law, 12(4), 2010.

[3]. Bigo, Didier and Carrera, Sergio and Hayes, Ben and Hernanz, Nicholas and Jeandesboz, Julien, "Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals", CEPS Paper in Liberty and Security in Europe, No. 52, December 2012.

[4]. Brouwer, Evelin, Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System, "Immigration and Asylum Law and Policy in Europe", vol. 15, Leiden, Martinus Nijhoff Publishers, 2008.

[5]. Coman, Iulian Marius, „Technology as Competitive Advantage in Intelligence and Facilitator of Security Cooperation", International Journal of Information Security and Cybercrime Vol. 7 Issue 1/2018.
[6]. Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA.
[7]. Council Decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC).
[8]. Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "EURODAC" for the comparison of fingerprints for the effective application of the Dublin Convention (EURODAC Regulation), OJ L 316, 15.12.2000.
[9]. Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention.
[10]. Council Regulation (EU) No 541/2010 of 3 June 2010 amending Regulation (EC) No 1104/2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II), OJ L 155, 22.6.2010.
[11]. Data Breach from January 2019 to April 2020, ENISA Threat Landscape December on the establishment, operation and use of the second generation Schengen.
[12]. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[13]. Dóczi, Zoltán, "The Development, the Integration and the Assessment of the Existing Large-Scale IT Systems in the Area of Freedom, Security and Justice", Acta Juridica Hungarica, 54(2), 2013.
[14]. Eu-LISA Annual Conference Report 2019, p.25.
[15]. EU-LISA Consolidated Annual Activity Report 2020, 29 June 2021.
[16]. Eu-LISA decision on Security Rules on the protection of CIS, 2019.
[17]. European Council Conclusions, 26/27 June 2014, Bruxelles.
[18]. Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, USA, 2018.
[19]. Good Practices in the Area of Border Security and Management in the Context of Counterterrorism and Stemming the Flow of "Foreign Terrorist Fighters", UNCCT, 2018 Information System (SIS II), OJ L 381, 28.12.2006.
[20]. IP/16/1247 "Stronger and Smarter Borders in the EU: Commission proposes to establish an Entry-Exit System", European Commission, Brussels, 6.4.2016.
[21]. MEMO/11/682 "Frequently Asked Questions: The Visa Information System goes live", Europa Press Releases RAPID, Brussels, 11.10.2011.
[22]. Protecting Large-scale IT systems developed and/or managed by eu-LISA from modern threats, eu-LISA, 2016.
[23]. Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II).
[24]. Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

[25]. Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.
[26]. Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011.
[27]. Regulation (EU) No 1052/2013 of the European Parliament and the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), OJ L 295, 6.11.2013.
[28]. Treaty of Lisbon amending the treaty on European Union and the treaty establishing the European Community, 2007/c 306/01.
[29]. Webpage: https://eucrim.eu/news/eu-creates-new-central-database-convicted-third-country-nationals/.
[30]. Webpage: https://www.eurocontrol.int/sites/default/files/content/documents/official-documents/forecasts/long-term-forecast-2010-2030.pdf.
[31]. Website: https://www.eulisa.europa.eu/Activities/Security.

Security Services in IP Networks

Marian-Ştefan GONCIULEA
University Politehnica of Bucharest, Romania
gonciulea.marian@yahoo.com

Abstract

In the field of information technology, network security is very important because many sensitive data are transmitted. Below you will find the important points we need to keep in mind when talking about security of a network: confidentiality, integrity, availability, authentication, and PKI – public key infrastructure.

Keywords: Confidentiality, Integrity, Availability, Authentication and Public Key Infrastructure

References

[1]. Octavian Catrina, Securitatea reţelelor şi serviciilor – note de curs.
[2]. https://www.giac.org/paper/gsec/2909/public-key-infrastructure-enabler-secure-trusted-computing/104903.
[3]. Octavian Catrina, Cryptographic Algorithms and Protocols.
[4]. CompTIA Security+ Certification Study Guide, Second Edition.
[5]. Octavian Catrina, Cryptography and Security in Communication Networks – note de curs.
[6]. https://www.giac.org/paper/gsec/2909/public-key-infrastructure-enabler-secure-trusted-computing/104903.

Legal Aspects Regarding Cybercrime

Virgil-Corneliu TUDOR
University Politehnica of Bucharest, Romania
virgilt2005@gmail.com

Abstract

In these days, cybercrime is an important phenomenon which involves two concepts: computers and networks. On the other hand, this fact can be usually called hacking. Some important examples are identity theft, espionage, credit card account thefts, online banking fraud and so on. Also, could be a dangerous risk in child pornography or when confidential information is intercepted. This article illustrates a lot of cyber-crime examples and the legal ways in order to protect the Internet users' safety.

Keywords: cybercrime, internet, legal

References

[1]. T. Amza, Criminologie, Suport de curs pentru învăţământ deschis la distanţă, Universitatea "Hyperion", Bucureşti, 2011, p.125.
[2]. http://www.juridice.ro/294005/ce-sondaj-privind-criminalitatea-informatica.html.
[3]. F. Encescu, Criminalitatea informatică, 2010.
[4]. I. Vasiu, Criminalitatea informatică, Nemira, Bucureşti, 1998, p.121-122.
[5]. T. Amza, Criminologie, Suport de curs pentru învăţământ deschis la distanţă, Universitatea "Hyperion", Bucureşti, 2011, p.121.
[6]. http://www.infoeuropa.md/criminalitatea-informatica/ „Criminalitatea informatică".
[7]. Art. 1 din Legea Nr. 20 din 03.02.2009 privind prevenirea şi combaterea criminalităţii informatice, publicat in Monitorul Oficial Nr. 11-12 la 26.01.2010.
[8]. http://www.securitatea-informatica.ro/criminalitatea-informatica/reglementari-privind-criminalitatea-informatica/.
[9]. http://www.criminalitate.info/.

Types of Cyber Attacks

Eduard-Alexandru NEDELCU
University Politehnica of Bucharest, Romania
nedelcueduardalexandru@yahoo.com

Abstract

One of the most exciting topics to learn about cyber security is the different types of attacks that hackers use to compromise systems and networks. This paper exposes the different types of attacks that are popular today and in some older attacks that have been popular in the past. The attacks come into categories—social engineering, network attacks, password attacks, and software attacks.

Keywords: cyber-attacks, hacker, e-mail, password

References

[1]. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/.
[2]. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.
[3]. https://www.rapid7.com/fundamentals/types-of-attacks.
[4]. https://www.sitelock.com/blog/2018/07/cyberattack-types/.
[5]. https://www.solarwinds.com/types-network-cyber-security-attacks.
[6]. https://www.blackstratus.com/7-types-cyber-attacks-small-medium-sized-businesses-face/.

Using AI to Defense Against Cybercrime

Andrei-Costin MIRON
University Politehnica of Bucharest, Romania
mironandreicostin@gmail.com

Abstract

Being one of the most rapidly expanding sectors, Internet has become one of the most vital part of our life from work to entertainment there's no other option now but it comes with a price of our privacy. Cybercrimes are also on the rapid expansion causing our sensitive data to be used without our permission. Governments are aware of this matter doing everything they can to secure our networks, but many say security is just an illusion. In this whole report we will analyse the strength of the people who are trying to spoil the Cyber Ecosystem and the higher grounds where we can deceive them.

Keywords: cybercrime, artificial intelligence, malware

References

[1]. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-2016-hate-crime-statistics.
[2]. http://www.encyclopedia.com/science-and-technology/computers-and-electrical-engineering/computersand-computing/internet-fraud.
[3]. https://www.cybrary.it/0p3n/types-of-hackers/.
[4]. Selma Dilek, Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review.

Cybercrime Phenomenon in Europe and Romania

Răzvan ZAMFIRACHE
University Politehnica of Bucharest, Romania
zamfirache.razvan@gmail.com

Abstract

Governments, the military, and the world economy can no longer work without the help of a computer. Computers that trade this huge amount of information communicate with each other via the Internet or through many other military or financial networks. Being a very important asset, information must be protected because it remains useful as long as it is valid, unaltered and true.

Keywords: cybercrime, cybersecurity, legislation

References

[1]. Gh. I. Ioniță, Infractiunile din sfera criminalitatii informatice, Editura Universul Juridic, 2012.
[2]. Ghid introductiv pentru aplicarea dispozitivelor legale referitoare la criminalitatea informatică, Internews Network.
[3]. http://mihaelabejenari.wordpress.com/criminalitatea-fara-violenta-fraudele-informatice/.
[4]. I. Vasiu, Criminalitate Informatica, Nemira, 2001.
[5]. http://ipn.md/ro/societate/57617.
[6]. http://unimedia.info/stiri/procuratura-vrea-sa-oblige-providerii-de-internet-sa-blocheze-site-urile-incomode-66610.html 20.
[7]. http://unimedia.info/stiri/dovada-proiectul-de-lege-privind-cenzura-internetului-contravine-mai-multor-standarde-europene-67004.html.
[8]. https://cepeoffice.wordpress.com/2012/08/20/cyber-security-an-important-dimension-of-romanias-national-security/.

An Analysis on Phishing Phenomenon

Antonia-Ruxandra CONSTANTIN
University Politehnica of Bucharest, Romania
antonia.constantin22@gmail.com

Abstract

This paper is about phishing, the simplest kind of cyberattack and, at the same time, the most dangerous and effective. At the beginning will be a presentation of what phishing is and how it works and after that how to prevent this type of cybercrime. Also, learning from examples is the best way, so a brief history of phishing attacks will show how people were really affected by it. The new trend is to digitalize everything in order to make our life easier. This means that security becomes very important because without it all the personal data and money can be stolen and never be recovered. This kind of attack can have a very big impact on big companies, not only on our personal data, so trainings and tests are scheduled periodically in order to prevent it.

Keywords: cyberattack, e-mail security, phishing techniques

References

[1]. https://www.webopedia.com/TERM/P/phishing.html.
[2]. https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html.
[3]. https://www.malwarebytes.com/phishing/.
[4]. https://www.webroot.com/nz/en/resources/tips-articles/what-is-phishing.
[5]. https://www.avast.com/c-phishing.
[6]. https://computer.howstuffworks.com/phishing.html.

Analysis of Computer Attacks

Adrian-Cristian PLOIEȘTEANU
University Politehnica of Bucharest, Romania
ploiesteanu.adrian@yahoo.com

Abstract

An cyberattack on computers or computer networks is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset. A cyber-attack is any type of offensive maneuver that targets computer information systems, infrastructures, computer networks, or personal computer devices. Cyber-attack is a sensitive issue in the world of Internet security. Governments and business organisations around the world are using various types of tools and techniques to keep the business running, while adversaries are trying to breach security and send malicious software such as botnets, viruses, trojans etc., to access valuable data. Every day the situation is getting worse because of new types of malware emerging to attack networks. It is important to understand those attacks both before and after they happen in order to provide better security to our systems. This paper presents the main attacks on computer systems and the ways of combating them.

Keywords: cyber-attack, malicious software, security

References

[1]. https://www.itgovernance.co.uk/blog/different-types-of-cyber-attacks.
[2]. https://www.wired.co.uk/article/ransomware-viruses-trojans-worms.
[3]. https://health.usf.edu/is/blog/2018/02/27/malicious-intentions-the-virus-worm--trojan.
[4]. https://blog.malwarebytes.com/threats/worm/.
[5]. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.
[6]. https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html.
[7]. https://www.kaspersky.com/resource-center/threats/adware.
[8]. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/.
[9]. https://searchsecurity.techtarget.com/definition/cross-site-scripting.
[10]. https://www.tpx.com/blog/cybersecurity-trends-2019/.
[11]. https://www.information-age.com/10-cyber-security-trends-look-2019-123463680/.

Research on Cybersecurity Education and Vulnerability Awareness in Educational Ecosystems

Daniela IONAȘC
"Principele Radu" Middle School, Adjud, Romania
dionasc@yahoo.com

Sabina-Daniela AXINTE
Faculty of Electronics, Telecommunications and Information Technology,
University POLITEHNICA of Bucharest, Romania
axinte_sabina@yahoo.com

Daniel BUCĂTARU
"A. T. Laurian" National College, Botoșani, Romania
bucatarudaniel@yahoo.com

Abstract

In the context of an abrupt migration of all daily activities towards online systems, due to the pandemic phenomenon and the long-delayed and dimmed investment in a national cybersecurity strategy, pupils, teachers and students alike were caught unprepared in an ominous and intricate environment. Due to the current context, the prevalence of medium- and high-complexity attacks has visibly increased, unveiling a need to research the level of awareness in the cybersecurity field for all parties included in the educational ecosystem: pupils, students, teachers and parents. This paper aims to gather inside information on their security education level by collecting and analyzing statistics related to the vulnerability awareness of all aforementioned stakeholders. Based on the results, mitigation plans will be proposed for each individual category, in corroboration with the most poignant problems and needs. The goal is to provide the necessary level of education for a safe and secure learning environment where future adults can focus on their evolutional growth.

Keywords: cybersecurity education, security awareness, safe and secure educational ecosystem

References

[1]. Eurostat Data Browser, General government expenditure by function, https://ec.europa.eu/eurostat/databrowser/view/gov_10a_exp/.
[2]. Status report of pre-university education in Romania, 2018, https://edu.ro/rapoarte-publice-periodice/.
[3]. PurpleSec Cyber Security Statistics https://purplesec.us/resources/cyber-security-statistics/.
[4]. State of vulnerabilities 2018-2019. Analysis of Events in the life of Vulnerabilities, ENISA, December 2019.
[5]. Kaspersky security research platform www.securelist.com.

[6]. Vulnerability awareness in educational ecosystem survey, https://docs.google.com/forms/d/e/1FAIpQLSfnQcQswZgcsOx7TWUedmejcT4w-8DkA_cuWi8D3oWF6pTK3g/viewform.

[7]. Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. Information Management & Computer Security, 18(5), 316–327. https://doi.org/10.1108/09685221011095236.

[8]. Annansingh, F., & Veli, T. (2016). An investigation into risks awareness and e-safety needs of children on the internet: A study of Devon, UK. Interactive Technology and Smart Education, 13(2), 147–165. https://doi.org/10.1108/ITSE-09-2015-0029.

[9]. Slusky, L., & Partow-Navid, P. (2012). Students Information Security Practices and Awareness. Journal of Information Privacy and Security, 8(4), 3-26, https://doi.org/10.1080/15536548.2012.10845664.

[10]. Considerations on Challenges and Future Directions in Cybersecurity, https://www.arasec.ro/documente/CybersecurityRO2019.pdf.

[11]. Neocortical Development. J Cogn Neurosci 1992; 4 (2): 175–176. doi: https://doi.org/10.1162/jocn.1992.4.2.175.

Author Guidelines

As an author, you are kindly advised to follow the next instructions. Reading and understanding the requirements before submittal would ensure adherence to the International Conference on Cybersecurity and Cybercrime standards and would facilitate acceptance by the scientific reviewers.

1. Papers must be submitted in English having an even number of pages (minimum 4 pages). At least 50% of the last page should be occupied by text.
2. For papers writing it is recommended the use the text processor Microsoft Word and one of the template models found on the conference website. We will do the final formatting and all necessary format conversions of your paper.
3. The papers will be submitted using our online interface. Please do not send your papers by email.
4. The papers will be reviewed by two scientific reviewers, well-known in their domains of activity. Usually, it takes 1 to 3 months between the moment you finished your submission and a response is given by scientific reviewers.
5. The papers will be sent back to the authors for corrections if the figures, pictures, or tables are not contained in the text or if the reviewers require modifications or supplementary information.
6. The papers will be rejected if their scientific content is not adequate, if they don't contain original elements and if they are not properly written in English.
7. The bibliography must show the authors adequate documentation. At least 7-10 quality references should be cited.
8. Citation standard is IEEE. Please read the IEEE Citation Reference from the website: www.ieee.org/documents/ieeecitationref.pdf.
9. The whole responsibility for the calculation exactitude, experimental data, scientific affirmation, and paper translation belongs to the authors.
10. The authors will declare on their own responsibility that the article or parts of it were not published before in other journals.

More information: https://proceedings.cybercon.ro/index.php/ic3/author-guidelines

The Romanian Association for Information Security Assurance (RAISA)

The Romanian Association for Information Security Assurance (RAISA) is a professional, non-governmental, non-partisan political, nonprofit, and public benefit association.

RAISA AIM

The aim of the Romanian Association for Information Security Assurance is promoting and supporting information security activities in compliance with applicable laws.

RAISA VISION

The vision of the Association is to promote research and education in information security field and to contribute to the creation and dissemination of knowledge and technology in this domain. RAISA has a strong representation at the national level, bringing together professors and researchers from top universities and Romanian institutions, PhD, master's, and license students, as well as companies in the IT segment.

RAISA OBJECTIVES

To achieve the stated purpose, the Romanian Association for Information Security Assurance proposes the following objectives:

- Collaboration with the academic community from Romania or abroad in order to organize conferences, scientific seminars and workshops for presenting the development and implementation of effective measures to improve information security.
- Collaboration with research centers, associations, and companies from Romania or abroad, to organize informative events in information technology security field.
- To perform specific programs for education and training of personnel involved in electronic information management (data processing, storage, security).
- To ensure the dissemination of notice relating to existing vulnerabilities and nationally and internationally newly identified threats; to provide solutions for data restoration and policies to prevent and combat incidents based on the information provided by suppliers of software solutions.
- To publish scientific journals for university staff, PhD students or master's students, researchers, students, and other professional categories in the field of information security and cybercrime.
- To grant awards, scholarships, or sponsorships to people with outstanding merits in the field of information security.

Website: www.raisa.org
Email: contact@raisa.org

RAISA Members Benefits

RAISA MEMBERS

The Romanian Association for Information Security Assurance (RAISA) is an organization that consists of:

- **Founding members** - are individuals who have participated in the founding process of the Association, have agreed with the Statute of the Association at the date of establishment and are parts of the members' category, with all their rights. The founding members pay annual membership fee and have the right to deliberative vote during the General Assembly.
- **Members** - are individuals who have joined the Association after the date of establishment. The members pay annual membership fee and have all the rights, respecting the obligations stipulated in Statute of the Association. They have the right to deliberative vote during the General Assembly.
- **Honorary Members** - can be scientists, professors, cultural or religious personalities, valuable professionals, who have rendered outstanding services to the Association. They are exempted from contributions and their vote is advisory.
- **Collaborators/Volunteers** - anyone who wants to participate in Association activities without becoming a member. Their collaborations are on no-cost basis; they don't pay a membership fee and don't have the right to vote.

RAISA MEMBERSHIP BENEFITS:

- Free access to RAISA events.
- Discount to workshops and conferences supported by RAISA.
- Discount for professional courses organized by RAISA.
- Possibility to be involved in RAISA projects and campaigns, support offered for research.
- Free publishing for scientific articles in the International Journal for Information Security and Cybercrime (IJISC), indexed in international databases.
- Discount for books and scientific studies promoted by RAISA.
- The possibility of promoting the events on RAISA media channels:
    - www.securitatea-cibernetica.ro
    - www.securitatea-informatiilor.ro
    - www.criminalitatea-informatica.ro

Get the most from your membership!

www.raisa.org/raisa-members/