Lecture Notes in Networks and Systems 990

The series “Lecture Notes in Networks and Systems” publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose (aninda.bose@springer.com).

Álvaro Rocha · Hojjat Adeli ·
Gintautas Dzemyda · Fernando Moreira ·
Aneta Poniszewska-Marańda
Editors

Good Practices and New Perspectives in Information Systems and Technologies

WorldCIST 2024, Volume 6

Springer

Editors
Álvaro Rocha
ISEG
Universidade de Lisboa
Lisbon, Portugal

Gintautas Dzemyda
Institute of Data Science and Digital Technologies
Vilnius University
Vilnius, Lithuania

Aneta Poniszewska-Marańda
Institute of Information Technology
Lodz University of Technology
Łódz, Poland

Hojjat Adeli
College of Engineering
The Ohio State University
Columbus, OH, USA

Fernando Moreira
DCT
Universidade Portucalense
Porto, Portugal

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-3-031-60327-3 ISBN 978-3-031-60328-0 (eBook)
https://doi.org/10.1007/978-3-031-60328-0

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

Preface

This book contains a selection of papers accepted for presentation and discussion at the 2024 World Conference on Information Systems and Technologies (WorldCIST'24). This conference had the scientific support of the Lodz University of Technology, Information and Technology Management Association (ITMA), IEEE Systems, Man, and Cybernetics Society (IEEE SMC), Iberian Association for Information Systems and Technologies (AISTI), and Global Institute for IT Management (GIIM). It took place in Lodz city, Poland, 26–28 March 2024.

The World Conference on Information Systems and Technologies (WorldCIST) is a global forum for researchers and practitioners to present and discuss recent results and innovations, current trends, professional experiences, and challenges of modern Information Systems and Technologies research, technological development, and applications. One of its main aims is to strengthen the drive toward a holistic symbiosis between academy, society, and industry. WorldCIST'23 is built on the successes of: WorldCIST'13 held at Olhão, Algarve, Portugal; WorldCIST'14 held at Funchal, Madeira, Portugal; WorldCIST'15 held at São Miguel, Azores, Portugal; WorldCIST'16 held at Recife, Pernambuco, Brazil; WorldCIST'17 held at Porto Santo, Madeira, Portugal; WorldCIST'18 held at Naples, Italy; WorldCIST'19 held at La Toja, Spain; WorldCIST'20 held at Budva, Montenegro; WorldCIST'21 held at Terceira Island, Portugal; WorldCIST'22 held at Budva, Montenegro; and WorldCIST'23, which took place at Pisa, Italy.

The Program Committee of WorldCIST'24 was composed of a multidisciplinary group of 328 experts and those who are intimately concerned with Information Systems and Technologies. They have had the responsibility for evaluating, in a 'blind review' process, the papers received for each of the main themes proposed for the conference: A) Information and Knowledge Management; B) Organizational Models and Information Systems; C) Software and Systems Modeling; D) Software Systems, Architectures, Applications and Tools; E) Multimedia Systems and Applications; F) Computer Networks, Mobility and Pervasive Systems; G) Intelligent and Decision Support Systems; H) Big Data Analytics and Applications; I) Human-Computer Interaction; J) Ethics, Computers & Security; K) Health Informatics; L) Information Technologies in Education; M) Information Technologies in Radiocommunications; and N) Technologies for Biomedical Applications.

The conference also included workshop sessions taking place in parallel with the conference ones. Workshop sessions covered themes such as: ICT for Auditing & Accounting; Open Learning and Inclusive Education Through Information and Communication Technology; Digital Marketing and Communication, Technologies, and Applications; Advances in Deep Learning Methods and Evolutionary Computing for Health Care; Data Mining and Machine Learning in Smart Cities: The role of the technologies in the research of the migrations; Artificial Intelligence Models and Artifacts for Business Intelligence Applications; AI in Education; Environmental data analytics; Forest-Inspired

Computational Intelligence Methods and Applications; Railway Operations, Modeling and Safety; Technology Management in the Electrical Generation Industry: Capacity Building through Knowledge, Resources and Networks; Data Privacy and Protection in Modern Technologies; Strategies and Challenges in Modern NLP: From Argumentation to Ethical Deployment; and Enabling Software Engineering Practices Via Last Development Trends.

WorldCIST'24 and its workshops received about 400 contributions from 47 countries around the world. The papers accepted for oral presentation and discussion at the conference are published by Springer (this book) in four volumes and will be submitted for indexing by WoS, Scopus, EI-Compendex, DBLP, and/or Google Scholar, among others. Extended versions of selected best papers will be published in special or regular issues of leading and relevant journals, mainly JCR/SCI/SSCI and Scopus/EI-Compendex indexed journals.

We acknowledge all of those that contributed to the staging of WorldCIST'24 (authors, committees, workshop organizers, and sponsors). We deeply appreciate their involvement and support that was crucial for the success of WorldCIST'24.

March 2024

Álvaro Rocha
Hojjat Adeli
Gintautas Dzemyda
Fernando Moreira
Aneta Poniszewska-Marańda

Organization

Conference

Honorary Chair

Hojjat Adeli	The Ohio State University, USA

General Chair

Álvaro Rocha	ISEG, University of Lisbon, Portugal

Co-chairs

Gintautas Dzemyda	Vilnius University, Lithuania
Sandra Costanzo	University of Calabria, Italy

Workshops Chair

Fernando Moreira	Portucalense University, Portugal

Local Organizing Committee

Bożena Borowska	Lodz University of Technology, Poland
Łukasz Chomątek	Lodz University of Technology, Poland
Joanna Ochelska-Mierzejewska	Lodz University of Technology, Poland
Aneta Poniszewska-Marańda	Lodz University of Technology, Poland

Advisory Committee

Ana Maria Correia (Chair)	University of Sheffield, UK
Brandon Randolph-Seng	Texas A&M University, USA

Chris Kimble	KEDGE Business School & MRM, UM2, Montpellier, France
Damian Niwiński	University of Warsaw, Poland
Eugene Spafford	Purdue University, USA
Florin Gheorghe Filip	Romanian Academy, Romania
Janusz Kacprzyk	Polish Academy of Sciences, Poland
João Tavares	University of Porto, Portugal
Jon Hall	The Open University, UK
John MacIntyre	University of Sunderland, UK
Karl Stroetmann	Empirica Communication & Technology Research, Germany
Marjan Mernik	University of Maribor, Slovenia
Miguel-Angel Sicilia	University of Alcalá, Spain
Mirjana Ivanovic	University of Novi Sad, Serbia
Paulo Novais	University of Minho, Portugal
Sami Habib	Kuwait University, Kuwait
Wim Van Grembergen	University of Antwerp, Belgium

Program Committee Co-chairs

Adam Wojciechowski	Lodz University of Technology, Poland
Aneta Poniszewska-Marańda	Lodz University of Technology, Poland

Program Committee

Abderrahmane Ez-zahout	Mohammed V University, Morocco
Adriana Peña Pérez Negrón	Universidad de Guadalajara, Mexico
Adriani Besimi	South East European University, North Macedonia
Agostinho Sousa Pinto	Polytechnic of Porto, Portugal
Ahmed El Oualkadi	Abdelmalek Essaadi University, Morocco
Akex Rabasa	University Miguel Hernandez, Spain
Alanio de Lima	UFC, Brazil
Alba Córdoba-Cabús	University of Malaga, Spain
Alberto Freitas	FMUP, University of Porto, Portugal
Aleksandra Labus	University of Belgrade, Serbia
Alessio De Santo	HE-ARC, Switzerland
Alexandru Vulpe	University Politechnica of Bucharest, Romania
Ali Idri	ENSIAS, University Mohamed V, Morocco
Alicia García-Holgado	University of Salamanca, Spain

Almir Souza Silva Neto	IFMA, Brazil
Álvaro López-Martín	University of Malaga, Spain
Amélia Badica	Universiti of Craiova, Romania
Amélia Cristina Ferreira Silva	Polytechnic of Porto, Portugal
Amit Shelef	Sapir Academic College, Israel
Ana Carla Amaro	Universidade de Aveiro, Portugal
Ana Dinis	Polytechnic of Cávado and Ave, Portugal
Ana Isabel Martins	University of Aveiro, Portugal
Anabela Gomes	University of Coimbra, Portugal
Anacleto Correia	CINAV, Portugal
Andrew Brosnan	University College Cork, Ireland
Andjela Draganic	University of Montenegro, Montenegro
Aneta Polewko-Klim	University of Białystok, Institute of Informatics, Poland
Aneta Poniszewska-Maranda	Lodz University of Technology, Poland
Angeles Quezada	Instituto Tecnologico de Tijuana, Mexico
Anis Tissaoui	University of Jendouba, Tunisia
Ankur Singh Bist	KIET, India
Ann Svensson	University West, Sweden
Anna Gawrońska	Poznański Instytut Technologiczny, Poland
Antoni Oliver	University of the Balearic Islands, Spain
Antonio Jiménez-Martín	Universidad Politécnica de Madrid, Spain
Aroon Abbu	Bell and Howell, USA
Arslan Enikeev	Kazan Federal University, Russia
Beatriz Berrios Aguayo	University of Jaen, Spain
Benedita Malheiro	Polytechnic of Porto, ISEP, Portugal
Bertil Marques	Polytechnic of Porto, ISEP, Portugal
Boris Shishkov	ULSIT/IMI - BAS/IICREST, Bulgaria
Borja Bordel	Universidad Politécnica de Madrid, Spain
Branko Perisic	Faculty of Technical Sciences, Serbia
Bruno F. Gonçalves	Polytechnic of Bragança, Portugal
Carla Pinto	Polytechnic of Porto, ISEP, Portugal
Carlos Balsa	Polytechnic of Bragança, Portugal
Carlos Rompante Cunha	Polytechnic of Bragança, Portugal
Catarina Reis	Polytechnic of Leiria, Portugal
Célio Gonçalo Marques	Polytenic of Tomar, Portugal
Cengiz Acarturk	Middle East Technical University, Turkey
Cesar Collazos	Universidad del Cauca, Colombia
Cristina Gois	Polytechnic University of Coimbra, Portugal
Christophe Guyeux	Universite de Bourgogne Franche Comté, France
Christophe Soares	University Fernando Pessoa, Portugal
Christos Bouras	University of Patras, Greece

Christos Chrysoulas	London South Bank University, UK
Christos Chrysoulas	Edinburgh Napier University, UK
Ciro Martins	University of Aveiro, Portugal
Claudio Sapateiro	Polytechnic of Setúbal, Portugal
Cosmin Striletchi	Technical University of Cluj-Napoca, Romania
Costin Badica	University of Craiova, Romania
Cristian García Bauza	PLADEMA-UNICEN-CONICET, Argentina
Cristina Caridade	Polytechnic of Coimbra, Portugal
Danish Jamil	Malaysia University of Science and Technology, Malaysia
David Cortés-Polo	University of Extremadura, Spain
David Kelly	University College London, UK
Daria Bylieva	Peter the Great St. Petersburg Polytechnic University, Russia
Dayana Spagnuelo	Vrije Universiteit Amsterdam, Netherlands
Dhouha Jaziri	University of Sousse, Tunisia
Dmitry Frolov	HSE University, Russia
Dulce Mourato	ISTEC - Higher Advanced Technologies Institute Lisbon, Portugal
Edita Butrime	Lithuanian University of Health Sciences, Lithuania
Edna Dias Canedo	University of Brasilia, Brazil
Egils Ginters	Riga Technical University, Latvia
Ekaterina Isaeva	Perm State University, Russia
Eliana Leite	University of Minho, Portugal
Enrique Pelaez	ESPOL University, Ecuador
Eriks Sneiders	Stockholm University, Sweden; Esteban Castellanos ESPE, Ecuador
Fatima Azzahra Amazal	Ibn Zohr University, Morocco
Fernando Bobillo	University of Zaragoza, Spain
Fernando Molina-Granja	National University of Chimborazo, Ecuador
Fernando Moreira	Portucalense University, Portugal
Fernando Ribeiro	Polytechnic Castelo Branco, Portugal
Filipe Caldeira	Polytechnic of Viseu, Portugal
Filippo Neri	University of Naples, Italy
Firat Bestepe	Republic of Turkey Ministry of Development, Turkey
Francesco Bianconi	Università degli Studi di Perugia, Italy
Francisco García-Peñalvo	University of Salamanca, Spain
Francisco Valverde	Universidad Central del Ecuador, Ecuador
Frederico Branco	University of Trás-os-Montes e Alto Douro, Portugal
Galim Vakhitov	Kazan Federal University, Russia

Gayo Diallo	University of Bordeaux, France
Gabriel Pestana	Polytechnic Institute of Setubal, Portugal
Gema Bello-Orgaz	Universidad Politecnica de Madrid, Spain
George Suciu	BEIA Consult International, Romania
Ghani Albaali	Princess Sumaya University for Technology, Jordan
Gian Piero Zarri	University Paris-Sorbonne, France
Giovanni Buonanno	University of Calabria, Italy
Gonçalo Paiva Dias	University of Aveiro, Portugal
Goreti Marreiros	ISEP/GECAD, Portugal
Habiba Drias	University of Science and Technology Houari Boumediene, Algeria
Hafed Zarzour	University of Souk Ahras, Algeria
Haji Gul	City University of Science and Information Technology, Pakistan
Hakima Benali Mellah	Cerist, Algeria
Hamid Alasadi	Basra University, Iraq
Hatem Ben Sta	University of Tunis at El Manar, Tunisia
Hector Fernando Gomez Alvarado	Universidad Tecnica de Ambato, Ecuador
Hector Menendez	King's College London, UK
Hélder Gomes	University of Aveiro, Portugal
Helia Guerra	University of the Azores, Portugal
Henrique da Mota Silveira	University of Campinas (UNICAMP), Brazil
Henrique S. Mamede	University Aberta, Portugal
Henrique Vicente	University of Évora, Portugal
Hicham Gueddah	University Mohammed V in Rabat, Morocco
Hing Kai Chan	University of Nottingham Ningbo China, China
Igor Aguilar Alonso	Universidad Nacional Tecnológica de Lima Sur, Peru
Inês Domingues	University of Coimbra, Portugal
Isabel Lopes	Polytechnic of Bragança, Portugal
Isabel Pedrosa	Coimbra Business School - ISCAC, Portugal
Isaías Martins	University of Leon, Spain
Issam Moghrabi	Gulf University for Science and Technology, Kuwait
Ivan Armuelles Voinov	University of Panama, Panama
Ivan Dunđer	University of Zagreb, Croatia
Ivone Amorim	University of Porto, Portugal
Jaime Diaz	University of La Frontera, Chile
Jan Egger	IKIM, Germany
Jan Kubicek	Technical University of Ostrava, Czech Republic
Jeimi Cano	Universidad de los Andes, Colombia

Jesús Gallardo Casero	University of Zaragoza, Spain
Jezreel Mejia	CIMAT, Unidad Zacatecas, Mexico
Jikai Li	The College of New Jersey, USA
Jinzhi Lu	KTH-Royal Institute of Technology, Sweden
Joao Carlos Silva	IPCA, Portugal
João Manuel R. S. Tavares	University of Porto, FEUP, Portugal
João Paulo Pereira	Polytechnic of Bragança, Portugal
João Reis	University of Aveiro, Portugal
João Reis	University of Lisbon, Portugal
João Rodrigues	University of the Algarve, Portugal
João Vidal de Carvalho	Polytechnic of Porto, Portugal
Joaquin Nicolas Ros	University of Murcia, Spain
John W. Castro	University de Atacama, Chile
Jorge Barbosa	Polytechnic of Coimbra, Portugal
Jorge Buele	Technical University of Ambato, Ecuador; Jorge Gomes University of Lisbon, Portugal
Jorge Oliveira e Sá	University of Minho, Portugal
José Braga de Vasconcelos	Universidade Lusófona, Portugal
Jose M. Parente de Oliveira	Aeronautics Institute of Technology, Brazil
José Machado	University of Minho, Portugal
José Paulo Lousado	Polytechnic of Viseu, Portugal
Jose Quiroga	University of Oviedo, Spain
Jose Silvestre Silva	Academia Military, Portugal
Jose Torres	University Fernando Pessoa, Portugal
Juan M. Santos	University of Vigo, Spain
Juan Manuel Carrillo de Gea	University of Murcia, Spain
Juan Pablo Damato	UNCPBA-CONICET, Argentina
Kalinka Kaloyanova	Sofia University, Bulgaria
Kamran Shaukat	The University of Newcastle, Australia
Katerina Zdravkova	University Ss. Cyril and Methodius, North Macedonia
Khawla Tadist	Morocco
Khalid Benali	LORIA - University of Lorraine, France
Khalid Nafil	Mohammed V University in Rabat, Morocco
Korhan Gunel	Adnan Menderes University, Turkey
Krzysztof Wolk	Polish-Japanese Academy of Information Technology, Poland
Kuan Yew Wong	Universiti Teknologi Malaysia (UTM), Malaysia
Kwanghoon Kim	Kyonggi University, South Korea
Laila Cheikhi	Mohammed V University in Rabat, Morocco
Laura Varela-Candamio	Universidade da Coruña, Spain
Laurentiu Boicescu	E.T.T.I. U.P.B., Romania

Lbtissam Abnane	ENSIAS, Morocco
Lia-Anca Hangan	Technical University of Cluj-Napoca, Romania
Ligia Martinez	CECAR, Colombia
Lila Rao-Graham	University of the West Indies, Jamaica
Liliana Ivone Pereira	Polytechnic of Cávado and Ave, Portugal
Łukasz Tomczyk	Pedagogical University of Cracow, Poland
Luis Alvarez Sabucedo	University of Vigo, Spain
Luís Filipe Barbosa	University of Trás-os-Montes e Alto Douro
Luis Mendes Gomes	University of the Azores, Portugal
Luis Pinto Ferreira	Polytechnic of Porto, Portugal
Luis Roseiro	Polytechnic of Coimbra, Portugal
Luis Silva Rodrigues	Polytencic of Porto, Portugal
Mahdieh Zakizadeh	MOP, Iran
Maksim Goman	JKU, Austria
Manal el Bajta	ENSIAS, Morocco
Manuel Antonio Fernández-Villacañas Marín	Technical University of Madrid, Spain
Manuel Ignacio Ayala Chauvin	University Indoamerica, Ecuador
Manuel Silva	Polytechnic of Porto and INESC TEC, Portugal
Manuel Tupia	Pontifical Catholic University of Peru, Peru
Manuel Au-Yong-Oliveira	University of Aveiro, Portugal
Marcelo Mendonça Teixeira	Universidade de Pernambuco, Brazil
Marciele Bernardes	University of Minho, Brazil
Marco Ronchetti	Universita’ di Trento, Italy
Mareca María Pilar	Universidad Politécnica de Madrid, Spain
Marek Kvet	Zilinska Univerzita v Ziline, Slovakia
Maria João Ferreira	Universidade Portucalense, Portugal
Maria José Sousa	University of Coimbra, Portugal
María Teresa García-Álvarez	University of A Coruna, Spain
Maria Sokhn	University of Applied Sciences of Western Switzerland, Switzerland
Marijana Despotovic-Zrakic	Faculty Organizational Science, Serbia
Marilio Cardoso	Polytechnic of Porto, Portugal
Mário Antunes	Polytechnic of Leiria & CRACS INESC TEC, Portugal
Marisa Maximiano	Polytechnic Institute of Leiria, Portugal
Marisol Garcia-Valls	Polytechnic University of Valencia, Spain
Maristela Holanda	University of Brasilia, Brazil
Marius Vochin	E.T.T.I. U.P.B., Romania
Martin Henkel	Stockholm University, Sweden
Martín López Nores	University of Vigo, Spain
Martin Zelm	INTEROP-VLab, Belgium

Mazyar Zand	MOP, Iran
Mawloud Mosbah	University 20 Août 1955 of Skikda, Algeria
Michal Adamczak	Poznan School of Logistics, Poland
Michal Kvet	University of Zilina, Slovakia
Miguel Garcia	University of Oviedo, Spain
Mircea Georgescu	Al. I. Cuza University of Iasi, Romania
Mirna Muñoz	Centro de Investigación en Matemáticas A.C., Mexico
Mohamed Hosni	ENSIAS, Morocco
Monica Leba	University of Petrosani, Romania
Nadesda Abbas	UBO, Chile
Narasimha Rao Vajjhala	University of New York Tirana, Tirana
Narjes Benameur	Laboratory of Biophysics and Medical Technologies of Tunis, Tunisia
Natalia Grafeeva	Saint Petersburg University, Russia
Natalia Miloslavskaya	National Research Nuclear University MEPhI, Russia
Naveed Ahmed	University of Sharjah, United Arab Emirates
Neeraj Gupta	KIET group of institutions Ghaziabad, India
Nelson Rocha	University of Aveiro, Portugal
Nikola S. Nikolov	University of Limerick, Ireland
Nicolas de Araujo Moreira	Federal University of Ceara, Brazil
Nikolai Prokopyev	Kazan Federal University, Russia
Niranjan S. K.	JSS Science and Technology University, India
Noemi Emanuela Cazzaniga	Politecnico di Milano, Italy
Noureddine Kerzazi	Polytechnique Montréal, Canada
Nuno Melão	Polytechnic of Viseu, Portugal
Nuno Octávio Fernandes	Polytechnic of Castelo Branco, Portugal
Nuno Pombo	University of Beira Interior, Portugal
Olga Kurasova	Vilnius University, Lithuania
Olimpiu Stoicuta	University of Petrosani, Romania
Patricia Quesado	Polytechnic of Cávado and Ave, Portugal
Patricia Zachman	Universidad Nacional del Chaco Austral, Argentina
Paula Serdeira Azevedo	University of Algarve, Portugal
Paula Dias	Polytechnic of Guarda, Portugal
Paulo Alejandro Quezada Sarmiento	University of the Basque Country, Spain
Paulo Maio	Polytechnic of Porto, ISEP, Portugal
Paulvanna Nayaki Marimuthu	Kuwait University, Kuwait
Paweł Karczmarek	The John Paul II Catholic University of Lublin, Poland

Pedro Rangel Henriques	University of Minho, Portugal
Pedro Sobral	University Fernando Pessoa, Portugal
Pedro Sousa	University of Minho, Portugal
Philipp Jordan	University of Hawaii at Manoa, USA
Piotr Kulczycki	Systems Research Institute, Polish Academy of Sciences, Poland
Prabhat Mahanti	University of New Brunswick, Canada
Rabia Azzi	Bordeaux University, France
Radu-Emil Precup	Politehnica University of Timisoara, Romania
Rafael Caldeirinha	Polytechnic of Leiria, Portugal
Raghuraman Rangarajan	Sequoia AT, Portugal
Radhakrishna Bhat	Manipal Institute of Technology, India
Raiani Ali	Hamad Bin Khalifa University, Qatar
Ramadan Elaiess	University of Benghazi, Libya
Ramayah T.	Universiti Sains Malaysia, Malaysia
Ramazy Mahmoudi	University of Monastir, Tunisia
Ramiro Gonçalves	University of Trás-os-Montes e Alto Douro & INESC TEC, Portugal
Ramon Alcarria	Universidad Politécnica de Madrid, Spain
Ramon Fabregat Gesa	University of Girona, Spain
Ramy Rahimi	Chungnam National University, South Korea
Reiko Hishiyama	Waseda University, Japan
Renata Maria Maracho	Federal University of Minas Gerais, Brazil
Renato Toasa	Israel Technological University, Ecuador
Reyes Juárez Ramírez	Universidad Autonoma de Baja California, Mexico
Rocío González-Sánchez	Rey Juan Carlos University, Spain
Rodrigo Franklin Frogeri	University Center of Minas Gerais South, Brazil
Ruben Pereira	ISCTE, Portugal
Rui Alexandre Castanho	WSB University, Poland
Rui S. Moreira	UFP & INESC TEC & LIACC, Portugal
Rustam Burnashev	Kazan Federal University, Russia
Saeed Salah	Al-Quds University, Palestine
Said Achchab	Mohammed V University in Rabat, Morocco
Sajid Anwar	Institute of Management Sciences Peshawar, Pakistan
Sami Habib	Kuwait University, Kuwait
Samuel Sepulveda	University of La Frontera, Chile
Sara Luis Dias	Polytechnic of Cávado and Ave, Portugal
Sandra Costanzo	University of Calabria, Italy
Sandra Patricia Cano Mazuera	University of San Buenaventura Cali, Colombia
Sassi Sassi	FSJEGJ, Tunisia

Seppo Sirkemaa	University of Turku, Finland
Sergio Correia	Polytechnic of Portalegre, Portugal
Shahnawaz Talpur	Mehran University of Engineering & Technology Jamshoro, Pakistan
Shakti Kundu	Manipal University Jaipur, Rajasthan, India
Shashi Kant Gupta	Eudoxia Research University, USA
Silviu Vert	Politehnica University of Timisoara, Romania
Simona Mirela Riurean	University of Petrosani, Romania
Slawomir Zolkiewski	Silesian University of Technology, Poland
Solange Rito Lima	University of Minho, Portugal
Sonia Morgado	ISCPSI, Portugal
Sonia Sobral	Portucalense University, Portugal
Sorin Zoican	Polytechnic University of Bucharest, Romania
Souraya Hamida	Batna 2 University, Algeria
Stalin Figueroa	University of Alcala, Spain
Sümeyya Ilkin	Kocaeli University, Turkey
Syed Asim Ali	University of Karachi, Pakistan
Syed Nasirin	Universiti Malaysia Sabah, Malaysia
Tatiana Antipova	Institute of Certified Specialists, Russia
TatiannaRosal	University of Trás-os-Montes e Alto Douro, Portugal
Tero Kokkonen	JAMK University of Applied Sciences, Finland
The Thanh Van	HCMC University of Food Industry, Vietnam
Thomas Weber	EPFL, Switzerland
Timothy Asiedu	TIM Technology Services Ltd., Ghana
Tom Sander	New College of Humanities, Germany
Tomasz Kisielewicz	Warsaw University of Technology
Tomaž Klobučar	Jozef Stefan Institute, Slovenia
Toshihiko Kato	University of Electro-communications, Japan
Tuomo Sipola	Jamk University of Applied Sciences, Finland
Tzung-Pei Hong	National University of Kaohsiung, Taiwan
Valentim Realinho	Polytechnic of Portalegre, Portugal
Valentina Colla	Scuola Superiore Sant'Anna, Italy
Valerio Stallone	ZHAW, Switzerland
Verónica Vasconcelos	Polytechnic of Coimbra, Portugal
Vicenzo Iannino	Scuola Superiore Sant'Anna, Italy
Vitor Gonçalves	Polytechnic of Bragança, Portugal
Victor Alves	University of Minho, Portugal
Victor Georgiev	Kazan Federal University, Russia
Victor Hugo Medina Garcia	Universidad Distrital Francisco José de Caldas, Colombia
Victor Kaptelinin	Umeå University, Sweden

Viktor Medvedev	Vilnius University, Lithuania
Vincenza Carchiolo	University of Catania, Italy
Waqas Bangyal	University of Gujrat, Pakistan
Wolf Zimmermann	Martin Luther University Halle-Wittenberg, Germany
Yadira Quiñonez	Autonomous University of Sinaloa, Mexico
Yair Wiseman	Bar-Ilan University, Israel
Yassine Drias	University of Algiers, Algeria
Yuhua Li	Cardiff University, UK
Yuwei Lin	University of Roehampton, UK
Zbigniew Suraj	University of Rzeszow, Poland
Zorica Bogdanovic	University of Belgrade, Serbia

Contents

1st Workshop on Data Privacy and Protection in Modern Technologies

1st Workshop on Railway Operations, Modeling and Safety

3rd Workshop on Digital Marketing and Communication, Technologies, and Applications

4th Workshop on Open Learning and Inclusive Education Through Information and Communication Technology

1st Workshop on Environmental Data Analytics

1st Workshop on AI in Education

1st Workshop on Artificial Intelligence Models and Artifacts for Business Intelligence Applications

1st Workshop on The Role of the Technologies in the Research of the Migrations

12nd Workshop on Special Interest Group on ICT for Auditing and Accounting

2nd Workshop on Data Mining and Machine Learning in Smart Cities

2nd Workshop on Enabling Software Engineering Practices Via Last Development Trends

Phishing Webpage Longevity

Ivan Skula and Marek Kvet(✉)

Faculty of Management Science and Informatics, University of Žilina,
Univerzitná 8215/1, 010 26 Žilina, Slovak Republic
`skula@dobraadresa.sk`, `marek.kvet@uniza.sk`

Abstract. Cybercriminals often spend considerable time preparing for phishing attacks, which surprisingly tend to last only a few hours. This short longevity is evident when older phishing links quickly become inaccessible, either taken down or flagged as malicious. While this benefits potential victims by shortening the effective risk period, it also poses a challenge for researchers aiming to track and analyze current phishing trends to develop effective countermeasures. Understanding the typical lifespan of phishing webpages is crucial for creating phishing data collection solutions. Our study involved monitoring phishing webpages from PhishTank and OpenPhish for three months while capturing their active/inactive status. Collected data had to undergo multiple steps - removing duplicate, incorrect, or non-relevant entries. The analysis focused on uncovering the phishing webpages' longevity, while the summary offered key findings. The study reveals that phishing webpages have a remarkably short active lifespan, with significant variations in the ratio of active to inactive pages across different periods. The initial rapid decrease by ≈12% in active phishing webpages is notable, dropping from 65% to 53% within the first five minutes and less than 40% remaining active after 24 h.

Keywords: phishing · webpage lifespan · statistics

1 Introduction

As organizations and governments advance on their journey of digitalization, the significance of online safety cannot be overstated. Over half (59%) of consumers are concerned about falling victim to a cyberattack and more than half of those who fall victim to a cyberattack report an impact on their personal finances [9]. Phishing, a prevalent form of online deception, harmfully impacts individuals and communities, making the study of its mechanisms - specifically, the lifespan of phishing pages - not just a technical pursuit. Phishing is, by number of victims, the most common type of cybercrime [5].

This study aims to explore the empirical evidence to understand how long phishing pages remain active post-deployment. Anti-Phishing Working Group (apwg.org) has been monitoring and reporting phishing webpages "uptime" from 2008 till 2014 in their half-yearly "Global Phishing Surveys". Though they

Á. Rocha et al. (Eds.): WorldCIST 2024, LNNS 990, pp. 215–226, 2024.
https://doi.org/10.1007/978-3-031-60328-0_21

reported the mean "uptime" value, they also reported the median "uptime" value as the distribution of the values is positively skewed. Skewness results from the fact that though a significant portion of phishing webpages have "uptime" in hours, some have it in weeks or even months, which shifts the mean "uptime" towards these extreme values. Median "uptime" values in the reported period (2008–2014) ranged from 5 h and 45 min to 19 h and 30 min, with both trends observed (decrease as well as increase). Mean "uptime" values were between ≈23 h and 73 h [1,2]. The last reported metric, from the second half of 2014, reported median "uptime" at ≈10 h (mean "uptime" was almost 30 h). Another research from 2007 reported 20 h as a median "lifetime", which was a figure very close to the number reported by APWG for H1/2008, at 19 h and 30 min. The mean "uptime" of 62 h was higher than the one reported by APWG (49 h 30 min) [8]. In regards to the webpage availability after a certain period, the figures vary, and researchers stated 66% [11] or 80% [3] of inactive webpages after the initial 24 h. Another study [7] reports only 25% of webpages being active after twelve days. The figures provided show the responsiveness and trends in phishing defense but don't fully capture the campaign's duration. Phishing campaigns often involve multiple domains or content migration between domains and IPs, especially after exposure and flagging [4].

The paper is organized as follows: Sect. 2 describes the approach taken to collect the phishing webpage data. In Sect. 3, we describe in detail the process of cleansing the collected data. 4th section summarizes the analysis performed and the gathered results before the last and concluding Sect. 5 summarizes the findings.

2 Data Collection Approach

The most important aspect of the feasible data source was the ability to gather suspicious phishing URLs as soon as they were observed and reported by internet users. The three most relevant sources identified were - PhishTank (phishtank.org), PhishStats (phishstats.info), and OpenPhish (openphish.com). All three sites provide a near real-time feed of phishing data. Due to the temporary unavailability of PhishStats, only PhishTank and OpenPhish data were collected and analyzed.

2.1 Solution for Collecting the Phishing Webpages Status

To collect and record the needed data, two separate tools were built *Identify* and *Verify*. The complete sequence of events from the initial phishing page deployment till its status capture by the tools is depicted in the diagram (Fig. 1).

1. Attacker deploys new phishing webpage (T_0)
2. A suspicious phishing webpage is observed by a user
3. User reports the suspicious webpage to OpenPhish or PhishStats (T_1)
4. *Identify* checks the phishing feed and records the new webpages (T_2)

5. *Verify* reads the new recorded suspicious URL in the database, navigates to the URL and captures its status - active or inactive (T_3)
6. *Verify* continues to read the suspicious webpage in a pre-determined time window until the page is observed as inactive.

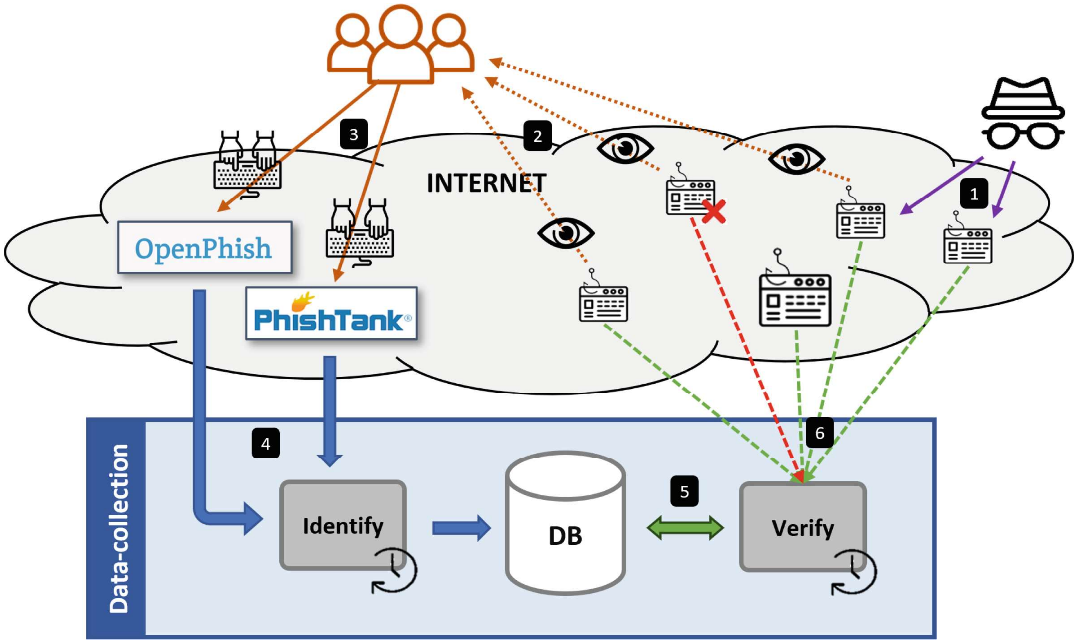

Fig. 1. Data collection process diagram.

Identify - was responsible for reading the data feeds every 2 min and recording new suspicious phishing URLs. This threshold was decided to balance the requirement to capture the status of phishing webpages as soon as possible with the impact of frequent reading on the underlying infrastructure. New records were saved into the database table, which utilized the uni-temporal structure of the destination table to capture the details while also separating inactive pages into the "HIST" table [6].

Verify - was periodically (every 10 s) monitoring the status of the records in the database and capturing the status if the record was new or the pre-defined time since the last status check has passed and during the last check, the webpage was still accessible (active). Verify stopped checking the status of those records that were inactive during the last status check (in practical terms, when the document size - HTML - read from the URL was zero, which meant it was removed or the hosting provider blocked the URL/site).
While in [8], authors were collecting the status every 30 min, APWG in [2] states that they were checking the status of the webpage several times per hour; we defined the following time windows at which the status was captured:

- immediately as the URL was recorded
- every hour within the first 24 h
- every day within the first 14 d
- 3rd and 4th week of first month
- 2nd - 6th, 9th and 12th month

Important Moments Within the Data Collection Process - from the (Fig. 1), four date and time points are observable, out of which three play an essential role in the analysis. The first is the moment(T_0) when the attacker deploys the phishing webpage and initiates the attack (via email, SMS, QR code, etc.). This exact moment is only known to the attacker and, for everyone else, remains unknown. It would be possible to capture this moment if we were able to capture the email or SMS used in the attack. This technique was successfully used in [10] and allows for a more precise measure of the attack duration. The next moment is when the user reports the observed suspicious webpage to PhishTank or OpenPhish (T_1), named SUBMISSION_DTTM. *Identify* can capture this moment only because PhishTank and OpenPhish share this information within their data feed. The following moment that *Identify* records is when it reads the data feed and identifies a new suspicious URL, which it records into the database table(T_2). This moment we named IDENTIFY_DTTM and serves as a primary reference moment for *Verify* when calculating the next time window for every individual phishing webpage. The last recorded moment (T_3) is when *Verify* reads and captures the status of the webpage after each pre-defined period passed. This moment was named VERIFY_DTTM and is recorded separately for each pre-defined time window.

3 Data Preparation

Data were collected during September, October, and November 2023 from two data sources - OpenPhish and PhishTank and only records with valid URLs were considered.

3.1 Confirmed Phishing URLs

As the users are reporting suspicious webpages, some are confirmed as phishing, and others are genuine webpages (also called False-Positives). PhishTank's final confirmation on the status of the reported phishing page requires manual review by more than one reviewer. So, many reported URLs are never closed as genuine or phishing. These undecided records, as well as those that were flagged as genuine webpages, had to be removed from the prepared dataset. OpenPhish also reports false positives, which were removed from the dataset but were rare. After this step the dataset shrank by nearly 23% from ≈219k records - ≈94K from OpenPhish and ≈125K from PhishTank - to ≈169k records out of which ≈93K originated from OpenPhish and ≈76K from PhishTank (Fig. 2).

3.2 Time-Delay Impact

As a result of the use of micro-batch execution in both components - Identify and Verify - varying delays in collecting the status of each recorder phishing webpage could have happened.

Delayed IDENTIFY_DTTM ($\mathbf{T_2}$) occurred when OpenPhish or PhishtTank placed the suspicious URL into the feed with delay on their side or when Identify failed to ingest the feeds as per schedule. This causes a widening gap between when the URL was reported to OpenPhish or PhishTank and when Verify could start recording the webpage status. After a quick data analysis, a *maximum threshold time gap of 10 min was defined.* More than 85% of the records fell within this threshold. Any record saved into our database later than 10 min after being recorded by OpenPhish or PhishTank (SUBMISSION_DTTM) was removed from the analysis. This condition ensures the analysis results are coupled with the earliest captured date and time(SUBMISSION_DTTM) and IDENTITY_TM is captured within a maximum of 10 min since SUBMISSION_DTTM.

Delayed initial VERIFY_DTTM ($\mathbf{T_3}$) occurred when Verify failed to capture the status shortly after the given time period for the webpage passed. Verify calculates the time passed since the IDENTIFY_DTTM only for those records seen as active in the previous check. If (for any reason) the status check doesn't happen, Verify will wait until it does. If, for example, Verify fails to record the webpage's status after two hours, it will not be able to update the status after three hours either, until the two-hour status is recorded - even if it happens many hours later. Verify can quickly recover and "catch up" with the current time window if the webpage is still active. However, if the webpage became inactive in between, such a record will not accurately capture when the page became inactive. To ensure consistency of the status capture, *a threshold of maximum delay was defined.* The maximum delay was breached if the Verify was supposed to capture the next time window, yet it is still missing the previous one. If, in this situation, inactive status is captured, it's impossible to decide whether the webpage became inactive in the current time window or the previous one. This ambiguity is relevant only if the most recent capture is inactive. Such records were, therefore, removed from analysis.

After applying the thresholds, the resulting dataset reduced by almost 27% to ≈124K records, out of which ≈77K were from OpenPhish and ≈47K from PhishTank (Fig. 2).

3.3 Duplicate Records Removal

Phishing attacks are often encountered by multiple users (Fig. 1), some of whom might report the attack to platforms like PhishTank or OpenPhish. As a result, the same domains are often reported repeatedly, leading to duplicate entries. To address this, we removed domains with identical elements up to the 5^{th}-level subdomain (chosen based on a prior analysis of domain granularity levels in our phishing data [12]), reported within 24 h from their first occurrence. This step resulted in a significantly reduced dataset. The resulting dataset shrank by 33% to ≈83K records - ≈56K from OpenPhish and only ≈27K from PhishTank (Fig. 2).

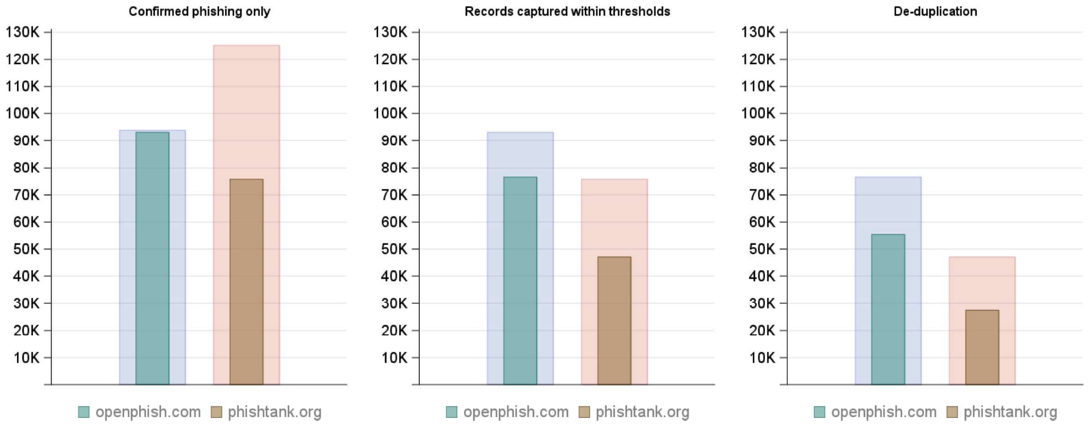

Fig. 2. Impact of data cleansing steps - confirmed phishing only (left), removal of records with delayed status capture (middle), and URL de-duplication (right). Before (bright) and after (dark).

3.4 Adjustment of Status for Small Pages

After a review of page sizes of captured records, we identified and decided to introduce a condition where all pages smaller than 200 bytes would be considered inactive. The size was based on an evaluation of a sample of pages of various sizes below 1000 bytes. The smallest phishing pages that used redirects were all slightly above 200 bytes. We found no webpage below 200 bytes, which was a valid phishing site. Most were pre-configured web server replies that the URL was unavailable or was taken down based on suspicion of being malicious. This rule improves the accuracy but doesn't fully correct the situation. There might still be webpages alerting users about the unavailability of the webpage on the domain, which might have more than 200 bytes.

The impact of this change was significant. Without adjustment, 31.2% of suspicious URLs collected by the Identify application were flagged as inactive during the initial status check. After the adjustment, this number grew to 40.2% (Fig. 3, last column ‘ALL’).

4 Phishing Webpages Longevity Analysis

Collected data were from a three-month period (Sep-Nov 2023), and so the volume of data decreases for weeks and months time-windows. The analysis was done in two parts to achieve the most accurate results based on the maximum number of applicable(mature) records. The *first* used all data with the age of at least *two weeks*. This way, the statistics used $\approx$82K records. The *second analysis* focused on the older data, *with the age of at least two months*. This analysis generated results while using approximately half of the records. Early results have shown that $\approx$40% (Fig. 4, row T) of suspicious webpages are inactive almost immediately after being captured from the data feed. To better understand this behavior, we conducted a separate analysis focusing on the first 10 min since the webpage is reported to OpenPhish or PhishTank (T_1=SUBMISSION_DTTM).

4.1 Longevity During the First Ten Minutes

The analysis compares the active vs. inactive webpages ratio within each of the first 10 min since SUBMISSION_DTTM. All records from the dataset had to be processed by the Identify application within 10 min of the SUBMISSION_DTTM as stated in data preparation section. This analysis grouped the records into buckets - "0.min" up to "9.min". Group "0.min" contains recorded suspicious URLs for which the initial status check happened within the 1st minute since the SUBMISSION_DTTM; group "1.min" contains URLs for which the status check happened between 1st and 2nd minute; and so on. Visualization of these groups (Fig. 3) and the ratio of active vs. inactive webpages in each group shows a visible trend where the ratio of inactive webpages grows slowly, minute by minute. In the first minute, 35.1% webpages are inactive; in the second, it's 38.3%; in the third, it's 39.4% and this trend continues up the fifth minute, topping at 44.2%. After that, the trends seem to stall, with some values higher and some lower. The important fact to consider here is the volume of records within each group. A green dotted line with correlating values on the right Y-axis represents this metric. The majority of the records are placed within the first five groups. Volume within the groups after "5.min" sharply decreases, which could explain why the trend doesn't copy the trend observed in the first five minutes.

4.2 Longevity Within First Two Weeks

A graphical representation of this analysis (Fig. 4) shows the gradual decrease of active webpages throughout the defined time windows. Only records older than two weeks were included in this analysis.

4.3 Longevity Within Months

This analysis could only consider records older than two months, as any "newer records" would still be yet to check their T+2m status. Collected data allowed us to analyze only three additional periods - T+3 weeks, T+4 weeks, and T+2 months. And since the set of data for this analysis would be only a subset of the data from previous analysis, we decided to build upon the figures from the above (first two weeks) analysis by applying a condition where only records with active status at the T+2 weeks($\approx$15K; 18.4% from 82K records) time-window

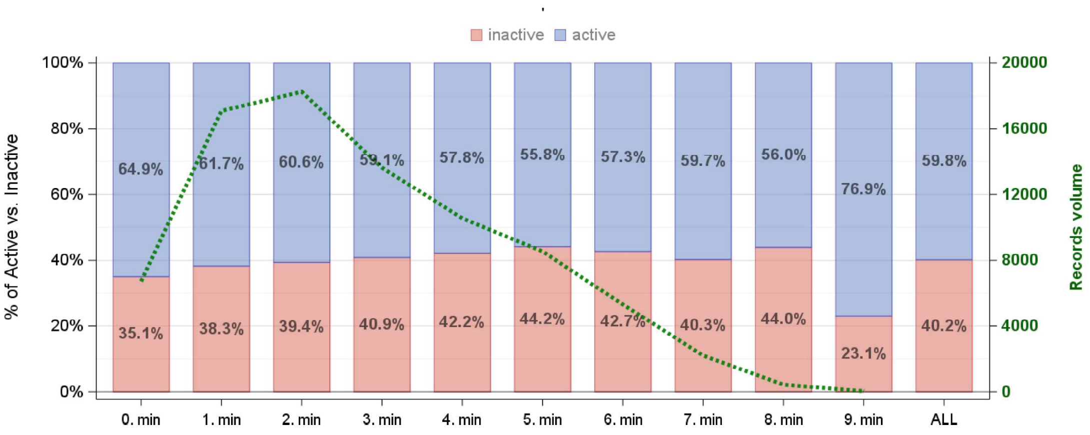

Fig. 3. Ratio of active vs. inactive phishing pages in each of initial 10 min and the overall ratio for all records

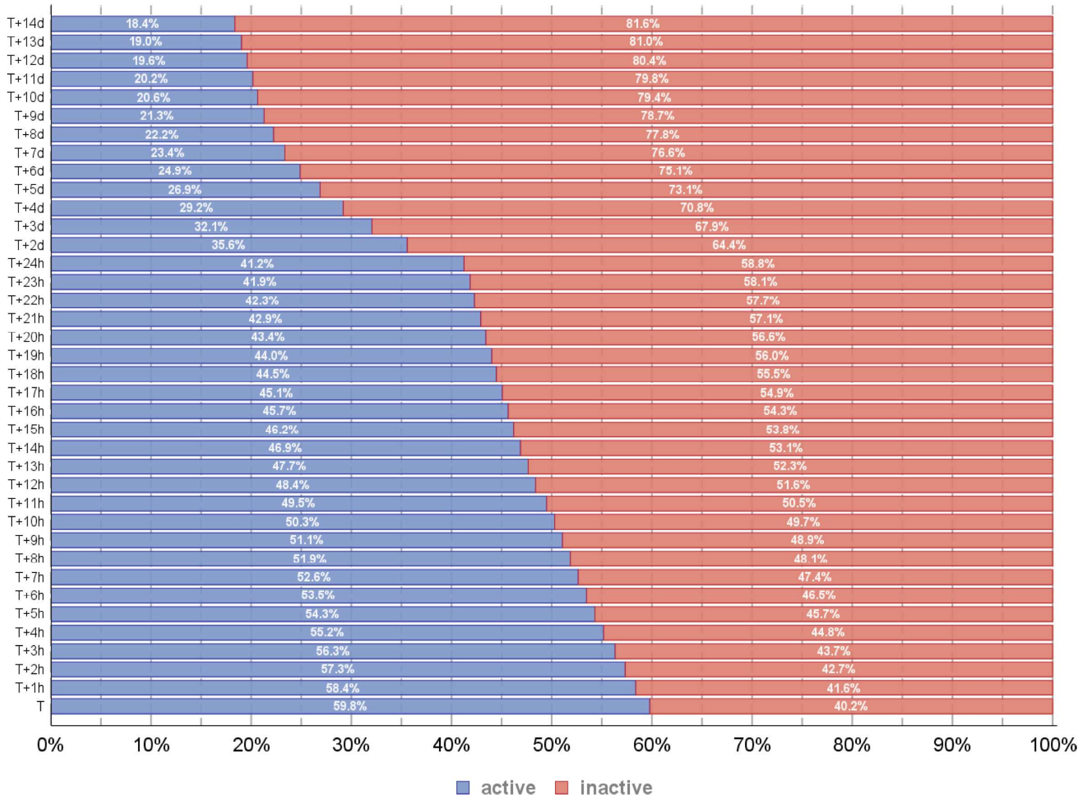

Fig. 4. Phishing webpage status - active vs. inactive ratio per time-window

check were considered and only those that were older than two months. After this filtering, the dataset had only ≈10K observations.

The final figures were as follows:

- T+3 weeks - 8.8% records became inactive from all active in T+2w
- T+4 weeks - 9.3% (additional 0.5%) inactive from all active in T+2w

- T+2 months - 15.5% (additional 6.2%) inactive from all active in T+2w

4.4 Volatility of Ratio Between Active and Inactive Webpages

As part of the review and validation process, we noticed that the ratio of active webpages varies a lot between different days. We, therefore, visualized the *daily ratio of active webpages through selected periods (T, T+24 h, and T+3 d)* to compare the change (Fig. 5). The bars on the graph are not stacked; each starts from 0% and reaches the height of the achieved ratio of active pages on a given day for a given time window. The blue dot within each day's column represents the volume of records on a given day to provide additional context. Volumes are linked to the values depicted on the right Y-axis of the graph. Daily mean number of records was ≈920, and all ≈83K records were considered.

The analysis confirmed the initial observation that the active webpages ratio at T (light-yellow color) varied from ≈44% (28th Of October) to ≈97% (3rd Of September - though the figure is based on less than 200 records) while mean value is ≈60% (Fig. 4). Figures at T+24 h (light-orange color) time window vary from ≈15% active webpages (26th Of October) to ≈71% (14th Of September) while mean value is ≈41%. Figures at T+3 d (dark-orange color) time window vary from ≈9% active webpages (7th Of November) to ≈68% (14th Of September) while mean value is ≈32%.

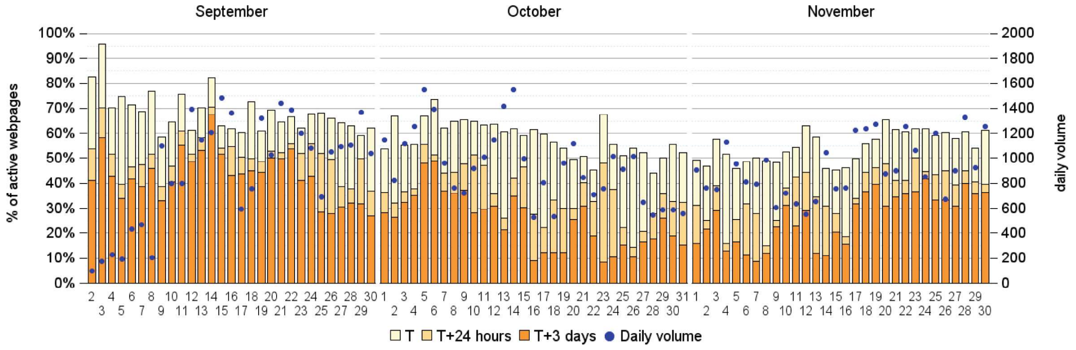

Fig. 5. Daily ratio of active webpages at T, T+24 h and T+3 d

4.5 Ratio of Active Webpages by the Source Data Feed

The analysis focused on comparing active webpages ratios between data collected from OpenPhish and PhishTank. Statistics were calculated for weekly as well as monthly periods. Both data feeds showed the same trends across the given period. The ratio for both PhishTank and OpenPhish gradually decreased from September to October and then gradually increased between October and November. Both data sources' figures copied this trend, and no opposing trends or notable differences were observed. Weekly active figures within the whole period ranged from ≈26% to ≈64%.

4.6 Median and Mean Lifespan of Active Webpage

Some articles that touched upon this topic calculated the mean and median lifespan of the phishing webpages, though they didn't provide a granular enough methodology to follow, which would allow for a direct comparison of figures. The data collection and cleansing process significantly impact the final (mean) figures, which is also why we described these steps in detail. All records - active and inactive were considered. The mean value was ≈224 h, which is approx. nine days and eight hours, but this number might increase as many records are older than two months and are still active. This figure is significantly higher than those reported by APWG in [1,2] and even higher than the high values mentioned in [8]. The median value, a more relevant metric, was only 10 h, the same as the last reported number by APWG [2] and lower than the figures reported in [8].

Comparing our figures with the stated webpages availability, we observed ≈60% of inactive pages after 24 h, similar to 66% [11]. After twelve days, we captured ≈20% webpages active, which is close to 25% [7].

5 Summary

Using the data from PhishTank and OpenPhish, the paper demonstrates that phishing webpages often have a very short active lifespan. To capture the details of phishing webpages, every minute matters, and availability drops rapidly (from 65% to 56% within the first five minutes). Approximately only 41% of reported phishing pages are active after 24 h, and only ≈36% after 48 h. However, the most significant finding is that 40% of the reported webpages are inactive when being collected from the data feed of PhishTank and OpenPhish. Focusing on the very first minute when the suspicious webpage is reported, already 35% of these URLs are inactive. Behind this relatively high number, there will be some that could be attributed to human error while reporting the suspicious webpage, some that could be a result of advanced techniques deployed on the phishing webpages to prevent scrapping or access from tools like curl. Some, which were removed as a result of tagging by anti-phishing solutions, but the question is how many were taken down by attacker as they achieved their objective?

Though the analysis is performed without the actual knowledge of the phishing webpage deployment date, it provides practical longevity figures for other researchers who plan to use data from OpenPhish or PhishTank. Based on this research, they can adapt their data collection strategy.

Not only having the actual real-world figures but also understanding the reasons behind them is crucial for optimizing the strategies for timely phishing prevention and detection. The transient nature of these sites poses challenges for real-time data collection and analysis. While the study provides a robust baseline for understanding phishing webpage longevity, it also emphasizes the need for continuous and rapid-response methodologies in cybersecurity research. Future studies could focus on extended periods beyond the two-month time window or assess the potential seasonal aspect of webpage longevity.

Acknowledgment. It was supported by the Erasmus+ project: Project number: 2022-1-SK01-KA220-HED-000089149, Project title: Including EVERyone in GREEN Data Analysis (EVERGREEN) funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the Slovak Academic Association for International Cooperation (SAAIC). Neither the European Union nor SAAIC can be held responsible for them.

Co-funded by the European Union

EverGreen DATA Analytics

References

1. Anti-Phishing Working Group: Global phishing survey: Trends and domain name use in 1h2009. Tech. rep., Anti-Phishing Working Group (2009). https://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf
2. Anti-Phishing Working Group: Global phishing survey: Trends and domain name use in 2h2014. Tech. rep., Anti-Phishing Working Group (2014). https://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_2H2014.pdf
3. Chu, W., Zhu, B., Xue, F., Guan, X., Cai, Z.: Protect sensitive sites from phishing attacks using features extractable from inaccessible phishing urls. In: IEEE International Conference on Communications (06 2013). https://doi.org/10.1109/ICC.2013.6654816
4. Cui, Q., Jourdan, G.V., Bochmann, G., Couturier, R., Onut, I.V.: Tracking phishing attacks over time. In: Proceedings of the 26th International Conference on World Wide Web Companion, pp. 667–676 (04 2017). https://doi.org/10.1145/3038912.3052654
5. FBI's Internet Crime Complaint Center: Internet Crime Report 2022. Tech. rep., FBI's Internet Crime Complaint Center (2022). https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
6. Kvet, M., Matiasko, K., Vajsova, M.: Sensor based transaction temporal database architecture. 2015 IEEE World Conference on Factory Communication Systems (WFCS), pp. 1–8 (2015). https://api.semanticscholar.org/CorpusID:19918990
7. McGrath, D.K., Gupta, M.: Behind phishing: An examination of phisher modi operandi. In: USENIX Workshop on Large-Scale Exploits and Emergent Threats (01 2008). https://api.semanticscholar.org/CorpusID:2069430
8. Moore, T., Clayton, R.: Examining the impact of website take-down on phishing. In: Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit 2007. vol. 269, pp. 1–13 (10 2007). https://doi.org/10.1145/1299015.1299016
9. Nationwide: September 2023 nationwide cybersecurity survey report. Tech. rep., Nationwide (2023). https://news.nationwide.com/download/bb78aae2-c720-4a7d-a6d8-423354c2cb53/cybersecurity-nationwidesurvey2023.pdf
10. Oest, A., et al.: Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In: 29th USENIX Security Symposium (USENIX Security 20), pp. 361–377. USENIX Association (08 2020). https://www.usenix.org/conference/usenixsecurity20/presentation/oest-sunrise

11. Sheng, S., Wardman, B., Warner, G., Cranor, L., Hong, J., Zhang, C.: An empirical analysis of phishing blacklists. International Conference on Email and Anti-Spam (07 2009). https://api.semanticscholar.org/CorpusID:1048051
12. Skula, I., Kvet, M.: Domain blacklist efficacy for phishing web-page detection over an extended time period. In: Proceeding of the 33rd Conference of FRUCT Association, pp. 257–263 (05 2023). https://doi.org/10.23919/FRUCT58615.2023.10142999