Pavlo Burda

Netherlands Italian, Ukrainian

p.burda@mailbox.org on request

www.pavlo.it @p_koelio paolokoelio

WORK EXPERIENCE

2018 – 2024

Doctoral Researcher in Information Security

Eindhoven University of Technology, Netherlands

Research as a Service coordinator between Threat Analysis group and IT department

Alignment of research directions between groups and proposition of a research program meeting mutual needs:

- evaluation of cyber-security organizational resilience (e.g., phishing assessments)
- data collection, analysis and infrastructure instrumentation for research (e.g., people and process analytics for organizational security)
- reports, recommendations and papers (e.g., measurements, policy assessments)

Supervisor and coordinator of scientific projects at MSc level

8 students resulting in 8 theses and 7 scientific publications on phishing vulnerability assessment, detection and mitigation.

Administrator of lab activities for Computer Networks & Security

Design and implementation of lab infrastructure for malware analysis (analysis environment, remote access and control) for 150+ students. Design and implementation of early-stage SOC for lab activities (Security Onion and Elastic Stack).

Instructor and teaching support for Operating Systems

Frontal instruction sessions with 200+ students. Coordinationf of Linux-based C programming assessments.

May – Oct 2017

Security Analyst

Communication Valley Reply, Milan

- C-SOC monitoring and incident analysis, vulnerability and patching management

2016 - 2017

Lecturer - Tutor

Volta College - University of Pavia, Italy

- Design and delivery of instructions for Computer Science, C, Python for web and LaTeX

HIGHLIGHTS AND IMPACT

Highlights

- Expertise in assessment of **phishing vulnerability** [9] [6], **attack features and user interaction** in Social Engineering (SE) [1] [4], technological [8] [10] and organizational **mitigation strategies** against phishing [3] [5] and **people analytics** for security [2].
- The **RaaS collaboration** contributed to the **adoption of MFA** and the uptake of **anti-phishing training** (embedded phishing exercises) and **mitigation** strategies (streamlining suspicious email reporting process) at TU/e.

Media

- Better resistance to phishing temptation - Cursor
- Pas op voor phishing op maat (Beware of tailored phishing) - Computer Idee

Seminars

- CISPA, Saarbrucken - 2023 - **Mapping human cognition to Social Engineering attacks: a research overview** (overview of the human attack surface)
- TU/e, Eindhoven - 2021 - **Human cognition and Social Engineering attacks** (interactions between social engineering and cognitive sciences) - IST Seminar
- UTwente, Enschede - 2019 - **Why does the weakest link fail: phishing experiments with humans** (phishing susceptibility and mitigation) - Risk & Resilience Festival
- TU/e, Eindhoven - 2019 - **Phishing experiments with humans: effectiveness of tailored phishing techniques** (tailored phishing vulnerability assessment) - EiPSI sem.

EDUCATION

2018 – 2024

PhD in Information Security - Speciality in Advanced Phishing

Eindhoven University of Technology, Netherlands

Title: Let the weakest link fail, but gracefully: understanding tailored phishing and measures against it [12]

Investigating the interactions between sophisticated phishing attacks, features of human cognition and organizational cyber security processes:

- characterizing and estimating risks of advanced phishing attacks
- developing organizational and technological mitigation strategies
- investigating interactions of human factors and organizational security processes

11 scientific publications spanning multiple disciplines including human computer interaction and technical communities

2015 – 2017

MSc in Computer Engineering

University of Pavia, Italy

- Thesis: Design and Implementation of a Forensic Triage Tool

2012 – 2015

BSc in Electronic and Computer Engineering

University of Pavia, Italy

- Thesis: General purpose server for remote sensor management, control and data viz.

SKILLS and EXPERIENCES

Technical experience

- **Phishing vulnerability assessment** - experience with academic research, RaaS
- **Tracking emerging threats, techniques and actors** - experience with academic research, tool creation, social engineering threat analysis and intelligence
- **People analytics for security** - quantitative and qualitative **data collection** for research (measurements, surveys and interviews) and **data analysis** in R
- **Python, C, JavaScript, Java, bash scripting** - experience with research, teaching, data collection and processing, tooling, personal projects
- **Linux and Windows administration** - implementing lab infrastructure and activities
- **AMTurk, AWS, Exchange API, web technologies** - experience with research, design of experiments, data pipelines, personal projects
- **InfoSec tools and techniques** - familiarity with network security software (SIEM, SMS, IPS, IDS), such as Qradar, Splunk, FireEye, Firesight and TippingPoint
- **Hacking tools** - familiarity using nmap, metasploit, wireshark and others, forensic software, OSINT techniques
- **Multimedia & Typesetting** - experience with producing content (Office, LaTeX, graphics)

Volunteering

2019 – 2022 **PhD Council** at TU/e - Mediating discussion points between TA colleagues and Department Board (e.g., periodic meetings, surveys, feedback)

2022 – 2023 **Foundation Ukrainians in the Netherlands** - Contact person at TU/e for UA student matters (e.g., interfacing with TU/e Board and Education Affairs, support cases, surveys)

Languages Italian, Ukrainian (mother tongues), English (professional proficiency), Czech, Polish (basic), Dutch (elementary)

Interests Sci-Fi, tennis, cyber warfare and fine food