



PhD in Information Technology and Electrical Engineering
Università degli Studi di Napoli Federico II

PhD Student: Gennaro Esposito Mocerino

Cycle: XXXIX

Training and Research Activities Report

Year: First

Tutor: prof. Alessio Botta

Date: October 31, 2024

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXIX

Author: Gennaro Esposito Mocerino

1. Information:

- PhD student: Gennaro Esposito Mocerino
 - DR number: DR997209
 - Date of birth: 12/01/1994
 - Master Science degree: Computer Engineering di Napoli Federico II
 - Doctoral Cycle: XXXIX
 - Scholarship type: no scholarship
 - Tutor: Prof. Alessio Botta
- PhD Cycle: XXXIX
- University: Università degli Studi

2. Study and training activities:

Activity	Type ¹	Hours	Credits	Dates	Organizer	Certificate ²
Strategic Orientation for STEM Research & Writing	Course	24	5	07-15/12/2023 12-19/01/2024 09-23/02/2024 04/04/2024	Sig.ra Adriana D'Auria – DIETI-Unina	Y
Video streaming on SP networks	Seminar	2	0.4	07/12/2023	Prof. Alessio Botta	Y
Energy-Efficient Data Science	Seminar	1	0.2	13/12/2023	prof. Elio Masciari, DIETI - Unina	Y
Hands-on Network Intrusion Detection via Machine and Deep Learning	Course	14	4	09-11-16-17-18/01/2024	dr. Antonio Montieri - DIETI-Unina	Y
IoT Data Analysis	Course	12	4	08-09-15-16-22-23/02/2024	prof. Raffaele Della Corte, DIETI	Y

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXIX

Author: Gennaro Esposito Mocerino

Using Deep Learning Properly	Course	12	4	23-25-30/01/2024 01-06-08/02/2024	dr. Andrea Apicella, DIETI-ITEE PhD	Y
Virtualization Technologies and their applications	Course	19	5	08-10-15-19-24-25-29-31/01/2024 05-07-26/02/2024	Prof. Luigi De Simone, DIETI - ITEE PhD	Y
Statistical data analysis for science and engineering research	Course	12	4	15-19-23-26-27-29/02/2024	Prof. Roberto Pietrantuono, DIETI-ITEE PhD	Y
Modellazione di sistemi con linguaggio UML	Seminar	2	0.4	16/04/2024	Prof. Beniamino Di Martino (UNICAMPANIA)	Y
High performance and cloud computing	Seminar	2	0.4	23/04/2024	Prof. Beniamino Di Martino (UNICAMPANIA)	Y
Big Data Architecture and Analytics	Course	20	5	06-07-13-14-16-20-21/05/2024	prof. Giancarlo Sperli - DIETI, Unina	Y
Free Virtual IEEE Authorship & Open Access Symposium	Seminar	2	0.4	07/05/2024	Dr. Petar Popovski, Eszter Lukács, Judy Brady (IEEE)	Y
Optimization of video transport over IP - Options and implementation in the Italian scenario	Seminar	2	0.4	29/05/2024	Prof. Alessio Botta (UNINA)	Y
Social Network	Seminar	2	0.4	07/06/2024	Prof.	Y

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXIX

Author: Gennaro Esposito Mocerino

Analysis: Methods and Applications	r			4	Giancarlo Sperli (UNINA)	
Introduction to Large Language Models Evolution and the current state	Seminar	2	0.4	10/06/2024	Prof. Giancarlo Sperli (UNINA)	Y
From ACE Technologies to Sustainable, Accessible and Equitable Urban Mobility: An Optimization Journey	Seminar	2	0.4	16/09/2024	Prof. Stefania Santini	Y
LLMs: teaching and learning (networking)	Seminar	2	0.4	18/09/2024	Prof. Jim Kurose – U. Massachusetts	N
IEEE Authorship and Open Access Symposium: Tips and Best Practices to Get Published from IEEE	Seminar	2	0.4	24/10/2024	Prof. Giovanni Ghione, Eszter Lukács, Judy Brady	Y

- 1) Courses, Seminar, Doctoral School, Research, Tutorship
- 2) Choose: Y or N

2.1. Study and training activities - credits earned

	Courses	Seminars	Research	Tutorship	Total
Bimonth 1	5	0.6	4	0	9.6
Bimonth 2	21	0	3	0	24
Bimonth 3	0	0.8	8	0	8.8
Bimonth 4	5	1.6	6	0	12.6
Bimonth 5	0	0	6	0	6
Bimonth 6	0	1.2	8	0	9.2
Total	31	4.2	35	0	70.2
Expected	30 – 70	10 - 30	80 - 140	0 – 4.8	

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXIX

Author: Gennaro Esposito Mocerino

3. Research activity:

In my first year as a PhD student, I dedicated a significant portion of my time studying and identifying the direction of my research. Through studying scientific literature and attending specialized courses and seminars, I discovered a critical challenge in the field of cybersecurity. This led me to focus on understanding and addressing the human factor in cybersecurity. The human element in security is often the weakest link, as it encompasses behavioral, psychological, and cognitive vulnerabilities that adversaries can exploit. In this context, human-centered cybersecurity investigates how human decision-making, and cognitive biases can be manipulated by attackers, making it a crucial area of study in the current threat landscape.

Recognizing the significance of this issue, I chose to focus specifically on phishing emails, given their critical impact within the broader cybersecurity domain. Phishing is a form of cyber-attack in which attackers impersonate trustworthy entities to trick individuals into divulging sensitive information or installing malicious software. It often relies on social engineering techniques that exploit cognitive vulnerabilities and emotional responses, making it a compelling area to explore the intersection between technology and psychology.

Allodi et al. (2019) highlight that the main challenge in countering phishing and social engineering attacks lies in the difficulty of current technologies to capture the human dimension inherent in these attacks [1]. Phishing attacks often exploit psychological mechanisms of human behavior, using principles of persuasion such as authority, reciprocity, and scarcity, as described by Cialdini to induce victims to act unconsciously or impulsively [2]. Current research has primarily focused on explicit detection methods, such as Spamley [3], which assesses the ability of users to identify phishing emails. Additionally, recent studies have explored how demographic factors can influence susceptibility to phishing and the effectiveness of various anti-phishing educational approaches [4].

Beyond technological aspects, it is therefore crucial to consider the human mind and its unconscious processes. In this regard, I focused on exploring the role of the unconscious mind in phishing attacks. The unconscious mind influences decision-making processes through implicit associations, which can significantly impact the detection of phishing emails. These implicit associations may lead users to overlook subtle cues that differentiate legitimate emails from phishing attempts, thereby increasing their susceptibility to such attacks.

To investigate this phenomenon, I am working on integrating psychological concepts with computer science by applying the Implicit Association Test (IAT) in the context of phishing emails. The IAT is a widely used psychological tool designed to measure implicit biases and associations that individuals may not be consciously aware of. It assesses the strength of automatic associations between mental representations of objects (e.g., "black" and "white").

First, I thoroughly studied the mechanics of the Implicit Association Test (IAT). One of the main studies on this topic was conducted by Ulrich Schimmack [5], who analyzed the statistical significance and scientific reliability of the results obtained through IAT. His findings emphasize that, particularly in

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXIX

Author: Gennaro Esposito Mocerino

the context of political orientation, implicit measurements align almost perfectly with explicit ones, suggesting high validity. The IAT has also been applied in the field of cybersecurity: for example, Rosanna di Gioia et al. [6] proposed using the IAT to educate children about cybersecurity risks, demonstrating promising results in raising risk awareness. However, the unconscious aspects of human thinking remain largely unexplored with respect to phishing.

Following this review, I developed a web application that allows users to take the test specifically in the context of phishing emails. The application consists of three parts: an initial survey, the IAT itself, and a final score with feedback. The survey collects anonymized data about the background of each user, including basic demographics, education, work experience, computer skills, and phishing awareness. These data points provide contextual information that will allow for more in-depth analysis in future studies, correlating IAT results with user characteristics.

The phishing-related IAT test I developed focused on several key persuasion principles frequently used in phishing attacks, such as reciprocity, urgency, authority, consistency, liking, and social proof. After building the platform, I conducted preliminary tests and obtained the following results:

Experts demonstrate a strong implicit association between phishing and urgency, as indicated by high and positive scores, which aligns with expectations in the field. Participants with moderate knowledge typically achieve medium to low positive scores. However, beginners often fail to recognize this implicit association, revealing a potential cognitive vulnerability that warrants further investigation. It is important to note that these are preliminary findings and require validation through a broader testing campaign. One of the key objectives for future research will be to scale up the testing and validate the results.

My overarching goal is to uncover hidden links between email elements and psychological vulnerabilities using the IAT. By analyzing linguistic styles, persuasion tactics, and cognitive biases, I aim to increase users' awareness and improve their ability to identify phishing attempts at a deeper cognitive level.

In addition to this platform, I worked on another platform, called Spamley, recently created with my research group to study another important aspect of phishing. This platform presents users with ten emails, asking them to determine whether each email is a phishing attempt or legitimate. Throughout the first year of my PhD, I renovated the front end of Spamley to align with contemporary technologies. Over the years, my research group and I have collected a significant amount of data from this platform. Currently, I am carrying out a systematic and thorough analysis of the collected data, utilizing suitable analytical tools and custom scripts.

In parallel to my primary research, I also contributed to two secondary projects in the field of AI and healthcare. The first project focused on the segmentation of electrocardiogram (ECG) signals using deep learning methods. This project has achieved promising results, which culminated in the publication of a paper that was accepted at a major conference.

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXIX

Author: Gennaro Esposito Mocerino

The second project involved analyzing tests performed by individuals with Parkinson's disease. I am currently processing and manipulating data for potential future developments, aiming to contribute to advancements in healthcare applications through AI.

References:

- [1] Allodi, L., Chotza, T., Panina, E., Zannone, N., 2019. *The need for new antiphishing measures against spear-phishing attacks. IEEE Security & Privacy* 18, 23–34.
- [2] R. B. Cialdini and R. B. Cialdini, *Influence: The psychology of persuasion*, vol. 55. Collins New York, 2007.
- [3] L. Gallo, D. Gentile, S. Ruggiero, A. Botta, and G. Ventre, "The human factor in phishing: Collecting and analyzing user behavior when reading emails," *Computers & Security*, vol. 139, p. 103671, 2024.
- [4] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI'10, (New York, NY, USA)*, p. 373–382, Association for Computing Machinery, 2010.
- [5] U. Schimmack, "The implicit association test: A method in search of a construct," *Perspectives on Psychological Science*, vol. 16, no. 2, pp. 396–414, 2021. PMID: 31647752.
- [6] Rosanna Gioia, Monica Gemo, Stephane Chaudron, and Ileana Di Pomponio. *Attitudes towards cyber risks implicit and self-report measures the happy on life edutainment experience of secondary school children*. 06 2019.

4. Research products:

Conference Papers:

- Gennaro Esposito Mocerino, Claudio Velotti, Danilo Gentile, Luigi Gallo, Alessio Botta, Giorgio Ventre, "Work in Progress: Implicit Association Tests for Understanding Human Factor in Phishing Beyond Awareness," in 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS\&PW), Vienna, Austria, 2024, pp. 519-526, doi: 10.1109/EuroSPW61312.2024.00063. – **published**
- Sayna Rotbei, Gennaro Esposito Mocerino, Muhammad Salman Haleem, Leandro Pecchia and Alessio Botta, "Detection of Heart Rhythm Parameters by Segmenting Electrocardiogram Signals," in 2024 IEEE-EMBS International Conference on Biomedical and Health Informatics, Houston, TX, USA, November 10-13, 2024 - **accepted**

Training and Research Activities Report

PhD in Information Technology and Electrical Engineering

Cycle: XXXIX

Author: Gennaro Esposito Mocerino

5. Conferences and seminars attended

- ITASEC24, The Italian Conference on CyberSecurity, organized by CINI's National Cybersecurity Laboratory, Salerno, April 8-11, 2024. Presentation of the Paper: "Beyond Awareness: Implicit Association Tests for understanding Human Factor in Phishing".
- 9th IEEE European Symposium on Security and Privacy, Vienna, July 8-12, 2024. Presentation of the Paper: "Work in Progress: Implicit Association Tests for Understanding Human Factor in Phishing Beyond Awareness"

6. Activity abroad:

I have not carried out any activity abroad during my first Ph.D. year.

7. Activity in partner companies:

I have not carried out any activity in partner companies

8. Tutorship

I have not carried out any tutorship during my first Ph.D. year