UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Dipartimento di Scienze Fisiche, Informatiche e Matematiche

The many faces of AI in the phishing-website landscape

Relatore: Dr. Giovanni Apruzzese
Affiliazione: University of Liechtenstein

Abstract. Phishing websites are everywhere. This fact may come at a surprise when considering the thousands of papers proposing artificial-intelligence (AI) techniques to counter this threat. Some of these techniques "work", i.e., they can reliably detect phishing websites---which is clearly an encouraging result. However, many "state-of-the-art" AI methods can also be trivially fooled with little effort by naive attackers---which is clearly a disheartening result. Finally, AI methods can also be offensively used by attackers to circumvent AI-based detectors---which is clearly a worrying result.

In this talk, I will explore these three complementary classes of results, each denoting a different "face" of AI. Specifically, I will explain on how AI can be used to catch phish. Then, I will show how to trivially evade these AI-based methods with simple modifications that anyone could do. Finally, I will reveal more sophisticated---but still affordable---ways to maliciously use AI tools to circumvent phishing detectors powered by AI. During this journey I will also emphasize the role of the end-user: ultimately, a phishing website must deceive a human---not an AI.

Time and location: December 17, 2024, 2 p.m.; Room L1.5, Building MO17 (Physics Building) Dept. FIM – Via Campi 213/b – Modena

Short bio. Giovanni Apruzzese is an Assistant Professor within the Hilti Chair of Data and Application Security at the University of Liechtenstein. He obtained the PhD in Information and Communication Technologies at the University of Modena and Reggio Emilia (Italy) in 2020. He authored over 30 peer-reviewed papers at internationally-recognized research venues. His research interests encompass a variety of themes, most of which revolve around cybersecurity and artificial intelligence. His primary expertise lies in network security and in phishing detection.

Host: Mauro Leoncini