

Nomination Statement

Dr. Edward Amoroso

The issue of human behavior and factors presents a major challenge to cybersecurity, as evidenced by the persistence of long-standing problems such as phishing attacks, which exploit human vulnerabilities even in the presence of advanced technologies. The recent World Economic Forum (WEF) Global Risks Report shows that 95% of all cybersecurity issues can be traced to human error [1]. As such, this problem is becoming the bottleneck of modern cybersecurity, with many attacks using social engineering techniques to enter and gain an initial foothold in networks.

This work recognizes the very importance of studying human vulnerabilities and developing defense technologies for human behaviors and cognition. Specifically, the research focuses on a class of innate human vulnerabilities that arise due to factors such as environmental stress, cognitive load, and habitual behaviors, leading to inattention and irrationality. Noticing that many people fall victims to phishing due to inattention, the authors answer a key question: *"How to guide the users' attention to proper email contents in real time, based on human data from biosensors, to improve their phishing recognition accuracy?"*

Compared to most of the existing works that analyze human data in a post-event manner, their work includes a set of transferable techniques that offer real-time evaluation and feedback control of attention processes, resulting in timely attention enhancement and improved accuracy of phishing recognition. In fact, experimental data shows that their approach enhances accuracy from 74.6% to a minimum of 86%. Moreover, online adaptive

learning and calibration further improve accuracy to 91.5% (resp. 93.7%) in less than 3 (resp. 50) learning stages.

The success of this research is attributed to the fruitful collaboration between a computer scientist and a psychologist who worked towards the ambitious goal of bridging experimentation and design. Their work is a pioneering achievement in the field of cybersecurity research, addressing the critical issue of human vulnerability in cybersecurity, an area that is still in its early stages. The study, accompanied by supplementary materials, including data deposited on the Open Science Framework (OSF) for open testing and benchmarking, lays the foundation for this critical field. It has the potential to become one of the seminal works in this area, with lasting impact for decades to come.

Moreover, this work holds great promise for the development of a successful startup focused on human-centric security. By further refining the research and transforming it into a tangible product, the startup could have a significant impact on the cybersecurity industry, helping to mitigate the persistent threat posed by phishing attacks and other forms of social engineering.

Reference: [1] The Global Risks Report 2022 17th Edition INSIGHT Report, Available at https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf