8-10-2020

Effect of Metacognition on Phishing Detection: Mediating Role of Situational Awareness

Nabid Alam
University of North Carolina at Greensboro, m_alam2@uncg.edu

Gurpreet Dhillon
IS and Supply Chain Management, gdhillon@uncg.edu

Effect of Metacognition on Phishing Detection: Mediating Role of Situational Awareness

TREO Talk Paper

Nabid Alam
UNC Greensboro
m_alam2@uncg.edu

Gurpreet Dhillon
UNC Greensboro
gdhillon@uncg.edu

Abstract

The Internet Crime Report by the Federal Bureau of Investigation states that the number of internet crime compliant reaches about half a million cases with reported loss exceeding 3.5 billion dollars in the year 2019 in the United States (US). Phishing attack or phishing scheme is one of the classes of internet crime. Phishing attack is broadly defined by unsolicited email, text, and telephone calls from imposter individual or business firm. Among all the reported cyberattack types in 2019 in the US, phishing scheme has the highest number of victims. According to the Federal Trade Commission, scammers carry phishing attacks primarily to steal internet user credentials, financial information, and social security information from the victims. The phishing attack victims report a loss totaling 57 million dollars in 2019 in the US. Thus, preventing this attack can reduce significant damage. Extant research on phishing attack prevention can be classified into two streams– focusing on the technological factor in phishing detection and focusing on the human factor in phishing detection. The technical stream deals with developing efficient automatic phishing detection systems by using algorithmic approaches and providing effective mitigation techniques after the detection. However, these techniques are effective when the phishing attack is not highly targeted. Focusing on the human factor is critical in phishing detection because human can deal with unique scenarios. When an attack reaches a user, then the user needs to safeguard themselves. The human factor stream of phishing detection deals with finding the reasons why technology users are susceptible to a phishing attack and making the users aware through training and communication to increase the likelihood of phishing detection at the users' side. Researches find that cybercriminals use persuasion techniques, emergency, and social pressure to attack the users. The user training and awareness studies investigate various approaches such as service policy, warning messages, educational notices, and mindfulness. Metacognitive knowledge, a psychological construct, usually deals with an individual's deeper thought process in any complex and dynamic decision-making environment. Existing literature provides little evidence on how metacognitive knowledge can be beneficial in the phishing detection by human. Thus, an extension of the current literature is to investigate the impact of metacognition in phishing detection. Metacognitive knowledge is vital in the context of phishing detection because it can make the users more aware of the threat. There are three main aspects of metacognitive knowledge, namely declarative knowledge, procedural knowledge, and conditional knowledge, and all these three impacts situational awareness. Situational awareness (SA) is defined by the perception about the environment, comprehension about the scenario, and projection about the future consequences. SA plays a crucial role in phishing because of the individual's need to assess the vulnerability and decide based on the situation. According to the Situational Awareness Theory (SAT), individual factors are antecedents of SA, and situational decision is a consequence of SA. Using SAT, we argue that an individual's level of metacognitive knowledge impacts phishing detection through the mediating role of situational awareness.