Understanding Cybersecurity Behavior in the Banking Industry Using Protection Motivation Theory

Virgino Agassie Dondokambey [a], Canitgia Tambariki [b], Octavianie Bernadette Sondakh [c], Evelyn Hendriana [d]

[abc] BINUS Business School Master Program, Bina Nusantara University, Jakarta, Indonesia
[d] BINUS Business School Doctor of Research in Management, Bina Nusantara University, Jakarta, Indonesia

ABSTRACT

The widespread adoption of digital technology has brought about significant transformations in various industries, including banking, where internet-based applications are used extensively for customer transactions. However, along with these advancements, there has been a parallel increase in cybercrime incidents, posing serious challenges for individuals and organizations. In Indonesia, this issue is particularly pronounced, with the country ranking as the eighth globally and the highest in Southeast Asia for the number of data breaches in 2022 (Dihni, 2022). Among the various forms of cybercrime, online fraud, such as phishing scams targeting banking customers, has become increasingly prevalent, leading to substantial financial losses (CNN Indonesia, 2022). In response to this alarming trend, regulatory bodies in Indonesia, including the Financial Services Authority and the Indonesian Central Bank, have devised a roadmap to strengthen IT security systems and mitigate cyber risks in the banking sector. While measures have been implemented to counter cybercrime risks, the perception of users regarding these threats often goes unnoticed. Previous research has primarily focused on individual awareness of cybercrime threats, overlooking the influence of perceived knowledge and protection habits on cybersecurity behavior (Shappie et al., 2019; Kimpe et al., 2021; Zwilling et al., 2022).

Keywords: Cybersecurity behaviour, Mobile banking, Perceived knowledge, Protection habit, Protection Motivation Theory (PMT)