ABSTRACT

In this digital era, information security and awareness of the risk of data leakage are very important aspects in the use of information technology, especially for confidential data. The use of Open Source Intelligence (OSINT) can help mitigate the risk of phishing attacks using technology-based methods by involving social engineering activities and implementing experiments using spear phishing techniques on email content. This can be utilized to identify security weaknesses that require improvement. This research includes implementation by utilizing OSINT, Social Engineering tools, and email content. Experiments involving OSINT and phishing attack are presented through Data Flow Diagram (DFD) to show the flow of the attack. Meanwhile, email content experiments are formulated using Activity diagrams that are applied for risk mitigation with technology-based methods. After that, based on the phishing attack, it is used to formulate risk mitigation on technology based. The risk mitigation is based on two technologies, namely email filters for email servers and two-factor authentication (2FA) for websites targeted by phishing attacks. By adding a two-factor authentication feature for websites that are targeted by phishing attacks because they have *input* in the form of account and password text boxes.

Keywords — ***OSINT, Phishing, Social Engineering, Technology Based***