ABSTRAK

Di era digital ini, keamanan informasi dan kewaspadaan terhadap risiko kebocoran data menjadi aspek yang sangat penting dalam penggunaan teknologi informasi, terutama untuk data yang bersifat rahasia. Penggunaan *Open Source Intelligence* (OSINT) dapat membantu mitigasi risiko *phishing attack* menggunakan metode *technology based* dengan melibatkan aktivitas *social engineering* serta implementasi eksperimen menggunakan teknik *spear phishing* pada konten *email*. Hal ini dapat dimanfaatkan untuk mengidentifikasi kelemahan keamanan yang memerlukan perbaikan. Penelitian ini mencakup implementasi dengan memanfaatkan OSINT, *Social Engineering tools*, dan konten *email*. Eksperimen yang melibatkan OSINT dan *phishing attack* disajikan melalui *Data Flow Diagram* (DFD) untuk menunjukkan alur dari serangan yang dilakukan. Sementara itu, eksperimen konten *email* dirumuskan dengan menggunakan *activity diagram* yang diterapkan untuk mitigasi risiko dengan metode *technology based*. Setelah itu, berdasarkan *phishing attack* tersebut digunakan untuk menyusun mitigasi risiko pada *technology based*. Mitigasi risiko tersebut berdasarkan dua teknologi yaitu filter *email* untuk *email server* dan autentikasi dua faktor (2FA) untuk *website* yang menjadi sasaran *phishing attack*. Dengan menambahkan fitur autentikasi dua faktor untuk *website* yang menjadi sasaran *phishing attack* karena memiliki *input* berupa *text box* akun dan *password*.

Kata kunci **— *OSINT, Phishing, Social Engineering, Technology Based***