

## INTISARI

Salah satu perkembangan teknologi saat ini itu yaitu berupa perkembangan jejaring media sosial, salah satunya adalah media sosial Instagram. Pendaftaran pada akun Instagram dapat menggunakan sebuah email. Email merupakan salah satu hasil dari perkembangan informasi dan komunikasi. Email banyak digunakan untuk bertukar informasi dengan mengirim dan menerima data, seperti file dokumen, gambar, surat dan lain-lain. Banyak kejahatan yang terjadi pada email. Kejahatan email yang bisa terjadi salah satunya yaitu email phishing. Email phishing merupakan tindakan memperoleh informasi data pribadi seperti username, password dan data-data sensitif lainnya dengan menyamar sebagai orang lain atau pihak yang berwenang melalui sebuah email. Kejahatan dunia maya melalui email pasti meninggalkan barang bukti seperti alamat IP, nama pengirim email, maupun domain pengirim email. Penelitian ini akan melakukan analisis forensik pada serangan email phishing menggunakan metode NIST (National Institute of Standards Technology). Penelitian ini bertujuan untuk membuktikan bagaimana metode NIST (National Institute of Standards Technology) dapat digunakan dalam mengidentifikasi serangan email phishing serta memberikan rekomendasi cara untuk melindungi pengguna agar terhindar dari serangan email phishing. Penelitian ini akan melakukan simulasi reka ulang adegan serangan email phishing dengan peneliti yang seolah-olah menjadi penyidik untuk menganalisis kasus serangan email *phishing* tersebut. Hasil dari penelitian ini penyidik berhasil mengidentifikasi serangan email *phishing* yang berisi informasi detail serangan dari hasil analisis menggunakan metode NIST (National Institute of Standards Technology). Penyidik juga berhasil menemukan perbandingan ciri-ciri antara email *phishing* dengan email resmi dari Instagram untuk dijadikan acuan pengguna Instagram agar terhindar dari serangan email *phishing*.

Kata kunci: Instagram, Email, Email Phishing, Forensic, NIST

## **ABSTRACT**

*One of the current technological developments is the development of social media networks, one of which is Instagram social media. Registration on an Instagram account can use an email. Email is one result of the development of information and communication. Email is widely used to exchange information by sending and receiving data, such as document files, images, letters and others. Many crimes that occur in email. One of the email crimes that can occur is phishing emails. Email phishing is an act of obtaining personal data information such as usernames, passwords and other sensitive data by posing as another person or an authorized party via an email. Cybercrimes via e-mail must leave evidence such as IP addresses, e-mail sender names, and e-mail sender domains. This research will conduct a forensic analysis of phishing email attacks using the NIST (National Institute of Standards Technology) method. This study aims to prove how the NIST (National Institute of Standards Technology) method can be used in identifying phishing email attacks and provide recommendations on how to protect users from phishing email attacks. This study will simulate the re-enactment of phishing email attack scenes with researchers who pretend to be investigators to analyze the phishing email attack cases. The results of this study investigators managed to identify phishing email attacks that contain detailed information on attacks from the results of analysis using the NIST (National Institute of Standards Technology) method. Investigators also managed to find a comparison of the characteristics between phishing emails and official emails from Instagram to be used as a reference for Instagram users to avoid phishing email attacks.*

*Keywords: Instagram, Email, Email Phishing, Forensics, NIST*