

ABSTRAK

E-banking adalah produk dari perkembangan *digital banking 4.0* yang menyediakan layanan yang memungkinkan nasabah bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik. Bank Rakyat Indonesia (BRI) juga mengeluarkan layanan *e-banking* yang bernama *BRI Mobile* (BRIMO) untuk mengikuti perkembangan *digital banking 4.0*. Perkembangan *e-banking* juga membuat kejahatan-kejahatan yang berkaitan dengan nasabah, bank dan pihak ketiga menjadi berkembang. Contoh kejahatan yang muncul akibat perkembangan *e-banking* adalah tindak kejahatan *phishing*. *Phishing* adalah salah satu bentuk kejahatan elektronik dalam bentuk penipuan dimana proses *phishing* ini bermaksud untuk menangkap informasi seperti *username*, *password* dan kartu kredit dalam bentuk menyerupai sebuah entitas yang dapat dipercaya/*legitimate organization* dan biasanya berkomunikasi secara elektronik. Tujuan dari penelitian ini adalah untuk mengetahui bagaimana pengaturan perundang-undangan tentang tindak kejahatan *phishing* dan untuk mengetahui bagaimana perlindungan yang diberikan BRI kepada nasabah agar nasabah terhindar dari tindak kejahatan *phishing*. Metodologi penelitian yang digunakan dalam skripsi ini adalah menggunakan metode pendekatan yuridis empiris, spesifikasi penelitian deskriptif analitis, metode pengumpulan sampel *purposive sampling* dan metode analisis data kualitatif.

Hasil dari penelitian ini menunjukkan bahwa belum ada pengaturan secara khusus tentang tindak kejahatan *phishing*. Pengaturan tentang kejahatan *phishing* masih menggunakan ketentuan yang ada pada Undang-Undang ITE dan KUHP. Perlindungan nasabah dari tindak kejahatan *phishing* merupakan tanggung jawab dari pemerintah dan pihak bank agar nasabah bank dapat mendapatkan rasa aman dari tindak kejahatan *phishing*.

Kata kunci: E-banking, BRI, Kejahatan Phishing

E-banking is a product of the development digital banking 4.0 which provides services that enable bank customers to obtain information, communicate, and carry out banking transactions through electronic media. Bank Rakyat Indonesia (BRI) also issued services banking named BRIMobile (BRIMO) to follow the developments of digital banking 4.0. Developments of e-banking also makes crimes that related to customers, banks and third parties develop. Examples of crimes that arise as a result of development of e-banking is a phishing crime. Phishing is a form of electronic crime in the form of fraud where the process of phishing intends to capture information such as username, password and credit cards in the form of resembling a trusted entity/legitimate organization and usually communicate electronically. The purpose of this research is to find out how the legislation regarding crime is regulate phishing and to find out how the protection provided by BRI to customers so that customers can avoid phishing. The research methodology used in this thesis is to use an empirical juridical approach, analytical descriptive research specifications, sample collection method purposive sampling and qualitative data analysis methods.

The results of this study indicate that there is no specific regulation regarding crime phishing. Crime setting phishing still using the existing provisions in the ITE Law and the Criminal Code. Protection of customers from crime phishing is the responsibility of the government and the bank so that bank customers can get a sense of security from crime phishing.