## ABSTRAK

Dunia saat ini tengah menghadapi masa pemulihan dari pandemi Covid-19 yang begitu dahsyat. Pandemi telah mengubah banyak hal utamanya perilaku masyarakat dalam bekerja dan menjalankan kehidupan. Kehadiran internet dan penciptaan *smartphone* sebagai alat untuk membantu masyarakat agar tetap aktif, lebih dari sekadar berkomunikasi dan mengakses informasi, namun juga menciptakan berbagai kemudahan dan manfaat dalam kehidupan. Pengembangan teknologi internet yang diterapkan pada industri perbankan terbukti mampu meningkatkan efisiensi dan menurunkan biaya operasional perusahaan. Selain itu, nasabah juga dimudahkan untuk melakukan transaksi online dimanapun dan kapan pun. Namun dibalik itu, keamanan data dan informasi menjadi isu utama penerapan teknologi internet dalam praktek perbankan. Ancaman kejahatan siber dalam praktek perbankan di Indonesia telah menjadi perhatian khusus bagi semua pihak. Salah satu dari modus kejahatan siber yang tidak pernah hilang karena adanya penegakan hukum adalah modus penipuan rekayasa sosial. Dengan memanfaatkan kelemahan manusia, penipuan rekayasa sosial selalu menimbulkan korban yang tidak sedikit dari tahun ke tahun. Mengantisipasi serangan psikologis pelaku penipuan rekayasa sosial tidak mudah karena sifat dan karakter manusia tidak sama. Selain itu kondisi dan orientasi manusia bisa berubah dari waktu ke waktu. Kondisi psikologis seseorang bisa terbentuk oleh lingkungan atau bisa muncul karena suatu rangsangan. Keterbatasan-keterbatasan inilah yang dimanfaatkan oleh pelaku. Pengaturan kejahatan siber modus penipuan rekayasa sosial diatur dalam KUHP, Undang-Undang ITE dan beberapa peraturan perundang-undangan yang lain. Terdapat hambatan-hambatan dalam penanganan modus tersebut yang diperlukan upaya khusus dari aparat penegak hukum untuk menanggulangi maraknya modus tersebut. Perbankan di Indonesia pada hakikatnya telah memiliki mekanisme dalam penanganan penipuan rekayasa sosial, namun tetap diperlukan adanya kesadaran yang tinggi bagi nasabah bank akan bahaya yang mengintai dari upaya para pelaku penipuan rekayasa sosial yang selalu mencari celah kelemahan para nasabah yang menyimpan dananya ke dalam rekening perbankan. Edukasi bank kepada nasabah tabungan untuk mengamankan dana yang disimpan dalam rekening beserta fitur teknologi yang melengkapinya belum cukup. Diperlukan kerjasama yang kuat dalam memerangi kejahatan siber dengan modus penipuan rekayasa sosial ini dari semua pihak. Antar perbankan, pemerintah atau regulator, aparat penegak hukum serta semua lapisan masyarakat yang mendukung adanya perlindungan hukum terhadap kejahatan siber dengan modus penipuan rekayasa sosial dalam praktek perbankan di Indonesia.


**Kata Kunci: Perlindungan Hukum, Kejahatan Siber, Penipuan Rekayasa Sosial, Bank.**

## *ABSTRACT*

*The world is currently facing a period of recovery from the devastating Covid-19 pandemic. The pandemic has changed many things, especially people's behavior in working and living their lives. The presence of the internet and the creation of smartphones as a tool to help people stay active, does more than just communicate and access information, but also creates various conveniences and benefits in life. The development of internet technology applied to the banking industry has proven to be able to increase efficiency and reduce company operating costs. In addition, it is also easier for customers to make online transactions anywhere and anytime. But behind that, data and information security is the main issue in the application of internet technology in banking practice. The threat of kejahatan siber in banking practices in Indonesia has become a special concern for all parties. One of the modes of kejahatan siber that never goes away due to law enforcement is the mode of penipuan rekayasa sosial. By exploiting human weaknesses, penipuan rekayasa sosial always causes many victims from year to year. Anticipating psychological attacks by penipuan rekayasa sosial actors is not easy because human nature and character are not the same. In addition, human conditions and orientations can change from time to time. A person's psychological condition can be formed by the environment or can arise due to a stimulus. These limitations are exploited by the perpetrators. The regulation of kejahatan siber mode of penipuan rekayasa sosial is regulated in the Criminal Code, the ITE Law and several other laws and regulations. There are obstacles in handling these modes which require special efforts from law enforcement officials to overcome the rampant modes. Banking in Indonesia essentially already has a mechanism in handling penipuan rekayasa sosial, but it is still necessary for bank customers to have high awareness of the dangers that lurk from the efforts of penipuan rekayasa sosial actors who are always looking for weaknesses in customers who deposit their funds into banking accounts. Bank education to savings customers to secure funds stored in accounts along with the technological features that complement them is not enough. Strong cooperation is needed in fighting kejahatan siber with this penipuan rekayasa sosial mode from all parties. Between banks, government or regulators, law enforcement officers and all levels of society that support legal protection against kejahatan siber with penipuan rekayasa sosial mode in banking practice in Indonesia.*


***Keywords: Legal Protection, Cyber Crime, Social Engineering, Banks.***