

**ANALISIS KESADARAN KEAMANAN INFORMASI PENGGUNAAN
LAYANAN M-BANKING OLEH PEGAWAI DINAS PERDAGANGAN,
PERINDUSTRIAN, DAN KOPERASI USAHA KECIL DAN MENENGAH
KABUPATEN BULELENG MENGGUNAKAN METODE HUMAN
ASPECTS OF INFORMATION SECURITY QUESTIONNAIRE (HAIS-Q)**

Oleh

Ngurah Gede Prema Satya Ananda, NIM 2015091047

Jurusan Teknik Informatika

ABSTRAK

Penelitian ini mengkaji masalah kesenjangan antara pemahaman dan praktik keamanan informasi pada pegawai Dinas Perdagangan, Perindustrian, dan Koperasi Usaha Kecil dan Menengah Kabupaten Buleleng dalam menggunakan layanan M-Banking yang rentan terhadap *phishing*. Tujuannya adalah untuk mengukur tingkat kesadaran keamanan informasi secara keseluruhan dan mengidentifikasi area terlemah sebagai dasar rekomendasi mitigasi yang lebih terfokus. Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei terhadap 119 pegawai. Instrumen penelitian dikembangkan berdasarkan kerangka Human Aspects of Information Security Questionnaire (HAIS-Q) untuk mengukur dimensi Pengetahuan, Sikap, dan Perilaku. Data yang terkumpul dianalisis menggunakan metode Multiple Weighted Score Analysis (MWSA) untuk menentukan skor dan peringkat kerentanan. Tingkat kesadaran keamanan informasi pegawai secara umum berada pada kategori “Baik” dengan skor 3,69. Meskipun demikian, temuan ini mengungkap adanya knowledge-attitude-behavior gap yang signifikan, dimana skor Pengetahuan dan Sikap yang tergolong “Baik” tidak diimbangi dengan skor dimensi Perilaku yang terkategori “Sedang”. Analisis perbandingan berdasarkan karakteristik responden menunjukkan bahwa pegawai pada kelompok usia produktif muda dan pengguna bank nasional cenderung memiliki skor kesadaran dan perilaku yang sedikit lebih tinggi dibandingkan kelompok usia produktif akhir dan pengguna bank daerah (BPD Bali). Untuk menjembatani kesenjangan ini, rekomendasi difokuskan pada pembuatan Standar Operasional Prosedur (SOP) yang dirancang sebagai alat untuk membentuk kebiasaan yang aman. Implementasi SOP ini didukung oleh kegiatan sosialisasi yang berorientasi pada perubahan perilaku, dan bukan sekadar penyampaian informasi. Dimana Sosialisasi ini perlu disertai pelatihan dan simulasi langsung, khususnya simulasi serangan *phishing*.

Kata - kata kunci: Keamanan Informasi, Kesadaran Keamanan, HAIS-Q, MWSA, M-Banking, Knowledge-Attitude-Behavior Gap.

AN ANALYSIS OF INFORMATION SECURITY AWARENESS OF MOBILE BANKING SERVICES USE BY EMPLOYEES OF THE DEPARTMENT OF TRADE, INDUSTRY, AND SMALL AND MEDIUM ENTERPRISE COOPERATIVES OF BULELENG REGENCY USING THE HUMAN ASPECTS OF INFORMATION SECURITY QUESTIONNAIRE (HAIS-Q)

By

Ngurah Gede Prema Satya Ananda, NIM 2015091047

Informatics Engineering Department

ABSTRACT

This research examines the gap between information security understanding and practice among employees of the Department of Trade, Industry, and Cooperatives for Small and Medium Enterprises of Buleleng Regency in utilizing M-Banking services, which are vulnerable to phishing. The objective is to measure the overall level of information security awareness and identify the weakest areas to serve as a basis for more focused mitigation recommendations. This study employs a quantitative approach using a survey method involving 119 employees. The research instrument was developed based on the Human Aspects of Information Security Questionnaire (HAIS-Q) framework to measure the dimensions of Knowledge, Attitude, and Behavior. Collected data were analyzed using the Multiple Weighted Score Analysis (MWSA) method to determine vulnerability scores and rankings. The results indicate that the general level of employee information security awareness falls within the "Good" category with a score of 3.69. Nevertheless, the findings reveal a significant knowledge-attitude-behavior gap, where "Good" scores in Knowledge and Attitude are not matched by the Behavior dimension, which is categorized as "Moderate." Comparative analysis based on respondent characteristics shows that employees in the young productive age group and users of national banks tend to have slightly higher awareness and behavior scores compared to the late productive age group and users of regional banks (BPD Bali). To bridge this gap, recommendations focus on the creation of Standard Operating Procedures (SOPs) designed as tools to cultivate secure habits. The implementation of these SOPs is supported by socialization activities oriented toward behavioral change rather than mere information delivery. Such socialization must be accompanied by direct training and simulations, specifically phishing attack simulations.

Keywords: *Information Security, Security Awareness, HAIS-Q, MWSA, M-Banking, Knowledge-Attitude-Behavior Gap.*