ABSTRAK

Nama	:	Ade Firman Fauzi
NIM	:	41517110172
Pembimbing TA	:	Leonard Goeirmanto, Dr., ST, M.Sc
Judul	:	Identifikasi Fake-Account Twitter Terhadap Social-Engineering Pretexting Pada Akun Bank Dan E-Wallet Di Indonesia Menggunakan Metode Naive Bayes, Neural-Network & SVM

Social Engineering merupakan teknik secara psikologis untuk memperoleh informasi data-data pribadi dengan cara memanipulasi korban. Salah satu teknik dalam Social Engineering dalam penelitian ini yaitu Teknik Pretexting, pada kasus ini, pelaku menggunakan identitas Palsu kemudian membuat serangkaian skenario atau dalih untuk meyakinkan korban untuk memancing korban memberikan data sensitif, seperti Email, Password, Nomor kartu, dan CSV. Kasus tersebut sering terjadi di era digital saat ini. Twitter salah satu saluran dimana perusahaan seperti perusahaan bank dan perusahaan dompet digital lainnya membuat akun resmi sebagai salah satu media penyaluran pelanggan, hal ini tentu menjadi celah bagi para kriminal dalam menjalankan aksi tersebut. Penelitian ini dibuat dengan tujuan untuk menganalisis akun Fake yang sering digunakan oleh para kriminal dalam teknik Pretexting.

Kami memperoleh data yang diduga merupakan kasus pretexting yang bersumber dari Twitter dan sebanyak 20 ribu data digunakan untuk proses klasifikasi. Data tersebut bersumber dari beberapa akun Bank dan Dompet digital di Indonesia. Penelitian ini menggunakan 3 algoritma klasifikasi yaitu Naive Bayes, SVM, dan Neural Network. Pada studi sebelumnya, parameter-parameter yang digunakan hanya menggunakan sosial parameter (jumlah following, followers, likes, etc) untuk mendeteksi akun palsu, namun pada penelitian ini penulis menambahkan parameter kata yang sering muncul dengan teknik TF-IDF. Sebagai hasil, Naive bayes memperoleh tingkat akurasi sebesar 96.3 % dengan data tanpa oversampling dan 98% dengan data oversampling. Penelitian ini menggunakan teknik SMOTE untuk menangani data oversampling.

Kata kunci - Akun palsu, Klasifikasi, Pretexting, Social Engineering

ABSTRACT

Name	:	Ade Firman Fauzi
Student Number	:	41517110172
Counsellor	:	Leonard Goeirmanto, Dr., ST, M.Sc
Title	:	Identifying Fake Accounts on Twitter Based on Social Engineering Pretexting in Indonesia Bank and E-wallet Accounts with Naive Bayes Neural Network, and SVM

Abstract - Social Engineering is a technique to obtain personal data information by manipulating victims. One of the techniques in Social Engineering in this research is the Pretexting Technique; in this case, the scammer uses a fake identity and makes scenarios or excuses to convince the victim to lure the victim into providing sensitive data, such as Email, Password, Card Number, and CSV.

Twitter is a channel where banks and other digital wallet companies create official accounts as customer relations, which is undoubtedly a gap for scammers to carry out these actions. The purpose of this study was to identify the fake account with pretexting tweets from several accounts in the bank and digital wallets from Indonesia in Twitter. This study uses three classification algorithms to identify fake accounts from bank accounts and other digital wallet accounts, especially in Indonesia. We compared Naive Bayes, SVM, and Neural Network. The previous study used social parameters (Number of followings, followers, likes, etc.) to detect fake accounts. Still, in this study, the authors added word parameters that often appear with the TF-IDF technique.

As a result, Naive Bayes obtained an accuracy rate of 96.3% with data without oversampling and 98% with oversampling data. This study uses the SMOTE technique to handle oversampling data.

Index Terms - classification, fake accounts, pretexting, social engineering