

**ANALISIS SERANGAN SOCIAL ENGINEERING MENGGUNAKAN METODE PRETEXTING,
IMPERSONATION DAN PHISING KEPADA PLAYER GAME MOBILE PUBGM & MOBILE
LEGENDS**



SKRIPSI

“Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Teknik
(S.Kom) Jenjang Pendidikan Strata-1”

Diajukan Oleh:

Nama: Valentinus Putra Setiawan

NIM : 2010101027

PROGRAM STUDI INFORMATIKA

UNIVERSITAS PRADITA

TANGERANG

TAHUN 2024

ABSTRAK

Penelitian ini menganalisis metode serangan rekayasa sosial (*social engineering*) yang terjadi dalam konteks permainan mobile *online*, khususnya pada *PUBG Mobile* dan *Mobile Legends*. Studi ini bertujuan untuk mengidentifikasi metode serangan seperti *pretexting*, *impersonation*, dan *phishing*, serta faktor-faktor yang mempengaruhi keberhasilannya. Penelitian dilakukan menggunakan metode kuantitatif, melibatkan simulasi serangan melalui platform media sosial, komunitas *game*, dan komunikasi dalam *game*. Hasil penelitian menunjukkan bahwa dari 124 responden yang menjadi target serangan, 88 akun berhasil ditembus. Faktor keberhasilan mencakup tekanan sosial, keterbatasan waktu bermain, rendahnya kesadaran pengguna terhadap risiko keamanan, dan daya manipulasi teknik *social engineering*. Sebaliknya, aktivasi fitur keamanan seperti autentikasi dua faktor (2FA) menjadi hambatan utama bagi keberhasilan serangan. Penelitian ini memberikan rekomendasi strategis untuk meningkatkan kesadaran dan perlindungan pengguna, termasuk edukasi keamanan digital, peningkatan fitur keamanan pada platform *game*, dan kolaborasi dengan komunitas *game*. Dengan implementasi langkah-langkah ini, risiko serangan *social engineering* dapat diminimalkan secara signifikan, menciptakan lingkungan *game* yang lebih aman bagi pemain.

Kata kunci: *Social Engineering, Pretexting, Impersonation, Phishing*

ABSTRACT

This study analyzes social engineering attack methods within the context of mobile online games, specifically PUBG Mobile and Mobile Legends. The research aims to identify attack methods such as pretexting, impersonation, and phishing, as well as the factors influencing their success. A qualitative methodology was employed, involving simulated attacks through social media platforms, gaming communities, and in-game communication. The findings reveal that out of 124 respondents targeted by these attacks, 88 accounts were successfully breached. Key success factors include social pressure, limited playing time, low user awareness of security risks, and the manipulative power of social engineering techniques. Conversely, the activation of security features such as two-factor authentication (2FA) served as the main barrier against successful breaches. This study offers strategic recommendations to enhance user awareness and protection, including digital security education, improved security features on gaming platforms, and collaboration with gaming communities. By implementing these measures, the risks associated with social engineering attacks can be significantly reduced, creating a safer gaming environment for all players.

Keywords: *Social Engineering, Pretexting, Impersonation, Phishing*

DAFTAR ISI

JUDUL.....	1
HALAMAN PERNYATAAN TIDAK PLAGIAT.....	5
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS	6
KATA PENGANTAR.....	7
ABSTRAK.....	9
ABSTRACT.....	9
BAB I	12
PENDAHULUAN	12
1.1 Latar Belakang	12
1.2 Rumusan Masalah	15
1.3 Batasan Masalah.....	15
1.4 Tujuan dan Manfaat Penelitian.....	16
1.5 Sistematika Penulisan	17
BAB I Pendahuluan.....	17
BAB II Tinjauan Pustaka.....	17
BAB III Metodologi Penelitian.....	17
BAB IV ANALISIS DAN PEMBAHASAN.....	17
BAB II.....	19
TINJAUAN PUSTAKA	19
2.1 Tinjauan Pustaka	19
2.2 Kerangka Teoritis	20
2.2.1 Social Engineering.....	20
2.2.2 Pretexting	21
2.2.3 Impersonation.....	21
2.2.4 Phishing	21
2.2.5 Game.....	22
2.2.6 Game Mobile Online	22
2.2.7 Komunitas Game	22
2.2.8 PUBGM	23
2.2.9 Mobile Legends	23
BAB III	25
METODOLOGI PENELITIAN.....	25
3.1 Metode Penelitian.....	25
3.2 Alur Penelitian.....	25

3.2 Metode Pengumpulan Data	26
3.3 Metode Serangan <i>Social Engineering</i> Yang Dipakai	31
3.3.1 Pretexting	31
3.3.2 Impersonation (Penyamaran).....	31
3.3.3 Phishing.....	31
3.4 Analisis	32
BAB IV	33
HASIL DAN PEMBAHASAN.....	33
4.1 Pengujian Pretexting.....	33
4.2 Pengujian Impersonation	41
4.3 Pengujian Phishing	50
4.4 Visualisasi dan Analisis Keberhasilan Metode Serangan	55
4.5 Visualisasi dan Analisis Usia Yang Terkena Serangan	58
4.6 Visualisasi dan Analisis Pendidikan Yang Terkena Serangan	60
BAB V	65
PENUTUP	65
5.1 Kesimpulan	65
5.2 Saran	Error! Bookmark not defined.