ANALISIS SISTEM PENIPUAN REKAYASA SOSIAL DENGAN KODE OTP (KASUS, PERETASAN MEDIA SOSIAL)

Dinda Destianti[1)], dan Moh. Nurjaman[2)]
[1,2)] Program Studi Sistem Informasi, Universitas Nusa Putra
Jl. Raya Cibolang No. 21 Cibolang Kaler, Cisaat, Sukabumi, Jawa Barat 43152
e-mail: dinda.destianti_si20@nusaputra.ac.id[1)], moh.nurjaman_si20@nusaputra.ac.id[2)]

* Korespondensi: e-mail: moh.nurjaman_si20@nusaputra.ac.id

ABSTRAK

Sistem yang umumnya kita gunakan sehari hari yang kita anggap aman dari berbagai ancaman kriminal seperti pencurian data dan hacking, sebenarnya masihlah rentan dan tidak seaman yang diketaui public. Pada kenyataan- ya penipuan penipuan masih sering terjadi di berbagai belahan dunia, khususnya di derah Indonesia sendiri. Penyerangan keamanan data pribadi dilakukan oleh kriminal dengan berbagai motif dan cara. Mulai dari cara yang paling mudah dan sederhana, hingga menggunakan cara yang cukup rumit dan memutar kepala. Itu semua dilakukan hanya untuk keuntungan diri mereka sendiri dengan merugikan banyak orang. Tapi tindak kriminal peretasan seperti itu bukanlah hal yang dapat dihentikan begitu saja. Karena pada dasarnya kejahahatan dan ke- baikan selalu berdampingan dalam kehidupan ini. Yang bisa kita lakukan hanyalah terus berhati hati dan tentu saja jangan jadi kejahatan itu sendiri. Kejahatan semacam ini atau umum disebut sebagai hacking merupakan ma- salah umum dan sering terjadi setiap harinya di kehidupan sehari hari. Ini karena perkembangan teknologi yang semakin maju dan semakin cerdas juga individu yang memperlajari teknologi. Namun sayangnya kecerdasan itu malah dijadikan sebuah tombak tajam untuk melakukan kejahatan, bukan malah menggunakannya untuk kebaikan dan kemajuan masyarakat. Dalam tulisan ini, kami akan coba menganalisa bagaimana system hacking yang dikhu- suskan pada media social seperti whatsapp dan penipuan melalui telepon seluler berjalan. Dan kami akan coba menguak cara seperti apa yang digunakan untuk melakukan kejahatan tersebut.

***Kata Kunci**: Kriminal, Penipuan, Hacking,Whatsapp, dan Telepon Seluler.*

ABSTRACT

The systems that we generally use on a daily basis that we consider safe from various criminal threats such as data theft and hacking, are actually still vulnerable and are not known to the public. In fact, fraud is still common in various parts of the world, especially in Indonesia itself. personal data security carried out by criminals with vari- ous motives and ways. Starting from the easiest and simplest way, to using a fairly complicated way and turning heads. It was all done only for their own benefit to the detriment of many people. But the crime of hacking like that is something that can be stopped just like that. Because basically evil and good always help in this life. All we can do is continue to be careful and of course not be a crime itself. This kind of crime or commonly referred to as hack- ing is a common problem and often happens every day in everyday life. This is because technological developments are increasingly advanced and smarter as well as individuals who study technology. But how lucky it is to become a sharp spear to commit crimes, not to be used for the progress and advancement of society. In this paper, we will try to analyze how hacking systems stored on social media such as whatsapp and through mobile phone fraud work. And we will try to uncover what methods were used to commit these crimes.

***Keywords**: Criminal, Theft, Haking, Whatsapp, and Mobile Phone.*

I. PENDAHULUAN

Dunia digital semakin berkembang seiring dengan berkembangnya teknologi digital yang sangat cepat dan maju. Tentu tantangan dalam berkembangnya pun tidak bisa dipungkiri bahkan kejahatan dunia digital semakin marak dan takterkendali. Berbagai jenis kejahatan terus menghantui para pengguna alat digital seperti masyarakat. Demi sebuah keuntungan dan tidakan yang tak bertanggung jawab. Tindak kejahatan kerap mengancam sebagian masyarakat pengguna teknologi digital. Belum lama ini terjadi modus penipuan baru di WhatsApp yang menyiasati pengguna untuk memberikan kode

OTP yang dikirim menggunakan huruf India. Taktik mengelabui dan memanipulasi korban ini dinamakan social engineering atau rekayasa sosial.

Rekayasa sosial adalah sebuah manipulasi psikologis yang dilakukan seseorang dalam melakukan aksi untuk menguak suatu informasi rahasia.

Dikutip dari Kaspersky, rekayasa sosial adalah sebuah teknik yang memanfaatkan kesalahan manusia untuk mendapatkan akses masuk, informasi pribadi dan data-data berharga. Jenis penipuan human hacking ini dapat memikat pengguna agar tak menaruh curiga kepada si penipu.

II. TINJAUAN PUSTAKA

A. Hacker dan Hacking

Hacking adalah sebuah Tindakan menemukan sebuah titik lemah atau entri dari sebuah sistem jaringan computer atau perangkat apapun yang terhubung dengan jaringan tanpa seizin pemilik. Lalu mengambil alih perangkat tersebut untuk kemudian dilakukan hal hal criminal yang bisa meruginakan seseorang yang terkena hacking tersebut.

Hacking biasanya dilakukan untuk mendapatkan akses tidak sah ke sistem komputer atau jaringan komputer, baik untuk membahayakan sistem atau mencuri informasi sensitif yang tersedia pada computer si korban.

Sedangkan Hacker adalah pelaku hacking itu sendiri. Hacker biasanya sangat pintar dan memiliki wa- wasan yang sangat luas terhadap bidang teknologi. Itu juga yang membuat Hacker menjadi pribadi yang sangat misterius. Karena dirinya menjadi berlebihan pintar dibidang itu. Hacker biasanya bekerja untuk dirinya sendiri atau bekerja pada perusahaan tertentu untuk menjaga keamanan data perusahaan tersebut.

Hacker umumnya dibagi menjadi dua kubu, yaitu white hat dan black hat. Sesuai Namanya. White hat artinya hacker yang putih, bersih dan baik hati. White hat biasanya adalah seorang programmer atau de- veloper. Sedangkan Black Hat adalah seorang hacker yang ingin disegani. Memiliki keinginan yang kuat untuk melakukan kejahatan. Dan bisanya bekerja dengan organisasi kejahatan.

B. Virus Komputer

Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus komputer dapat dianalogikan dengan virus biologis yang menyebar dengan cara menyisipkan dirinya sendiri ke sel makhluk hidup.

Virus computer cukup berbahaya dan bisa terdapat dimana saja. Jenisnya pun ada berbagai macam. Seperti kasus yang dulu pernah ramai pada sekitar tahun 2019, virus wannacry menyerang dunia. Jika computer anda terkontaminasi virus itu, maka Virus itu akan mengenkripsi seluruh data anda dan me- nyuruh anda untuk membeli ekriptornya dengan harga yang sangat tinggi jika mau menyelamatkan data anda yang terkena enkripsi tersebut.

Virus computer bisa menyebar lewat hal hal se sederhana situs web dan iklan iklan yang biasanya ada di situs situs dewasa dan berbagai situs perjudian online.

C. Phising

Phising adalah upaya untuk mendapatkan informasi data seseorang dengan teknik pengelabuan. Data yang menjadi sasaran phising adalah data pribadi berupa KTP, No Rekening dan berbagai data diri yang memiliki hubungan erat dengan keuangan. Phising sangat umum terjadi dibanding kejahatan lain. Contoh sederhananya adalah orang orang yang tertipu dengan sebuah postingan whatsapp yang berisikan pemba- gian kuota secara gratis dengan menyantumkan link pendaftaran yang misterius.

Cara kerjanya cukup sederhana, karena hanya dengan mengklik link yang tersedia lalu anda memasukan data diri anda disana maka secara tidak langsung data anda akan dikirim secara langsung ke database si penipu. Yang nantinya data itu akan digunakan untuk kepentingannya sendiri dan berbagai kejahatan lainnya .

D. Penipuan

Penipuan berbasis rekayasa sosial sebenarnya sudah terjadi sebelum teknologi secanggih sekarang. Hasil kajian Pusat Studi Masyarakat Digital Universitas Gadjah Mada (UGM), mengatakan bahwa mo- dus-modus itu sudah hadir sejak teknologi masih berada di era klasik berbasis e-mail, handphone, dan SMS.

Namun semenjak teknologi semakin advance (maju) tindakan para penipu mulai bergeser dari mengakses sistem menjadi memanipulasi psikologis pengguna. (Adityo hidayat, Cfds UGM). Pada peri- ode 2013-2017 modus penipuan berbasis rekayasa sosial rata-rat menggunakan topik undian berhadiah, advancefee scam, peretasan e-mail perusahaan, pemalsuan website , phising, dan “mamah minta pulsa”.

Pada 2018 topik manipulasi psikologis mulai berkembang dengan meminta akses kode OTP untuk transaksi finansial para korban dan meminda verifikasi penyedia jasa telekomunikasi melalui sms atau telepon.

Pada 2019 strategi pun berkembang dengan menghubungi pengguna dompet elektronik untuk mendapatkan OTP dengan kedok mendapat hadiah atau modus penipuan dengan meminta kode aplikasi olah pesan hingga call forwarding.

Kode OTP adalah kode verifikasi atau kata sandi sekali pakai yang biasanya terdiri dari 6 digit karakter yang sering kali berupa angka unik. Biasanya, OTP dikirimkan melalui sms atau e-mail dan umumnya berlaku untuk waktu yang sangat pendek misalnya 2 menit.

III. METODOLOGI PENELITIAN

A. Bahan

Bahan bahan yang digunakan cukuplah sederhana, karena kita hanya akan menganalisa bagaimana sistem peretasan dilakukan, bahan yang dipersiapkan tentunya hanya berupa seperangkat komputer lengkap dengan mouse, keyboard, monitor dan tentunya koneksi internet. Bahan lainnya hanya tambahan, bisa berupa ponsel dan kartu SIM Perdana yang tidak digunakan.

B. Metode Analisis Data

Analisis data digunakan dengan metode studi pustaka dengan cara mempelajari referensi- referensi bu- ku, jurnal, artikel dan browsing internet. Serta literature review yang berhubungan dengan analisis sistem. Pengumpulan data dengan mencari sumber sumber berita yang mendeskripsikan suatu objek kasus terkai- tan penelitian. sekilas contoh kasus seperti pada bab 1 pendahuluan dan penomena saat ini dengan berkembangnya kasus tersebut.

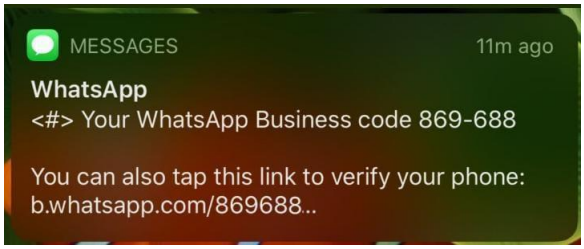
C. Fokus penelitian

Penelitian berfokus pada cara bagaimana mengetahui sistem penipuan berbasis rekayasa sosial ini beker- ja.

IV. HASIL DAN PEMBAHASAN

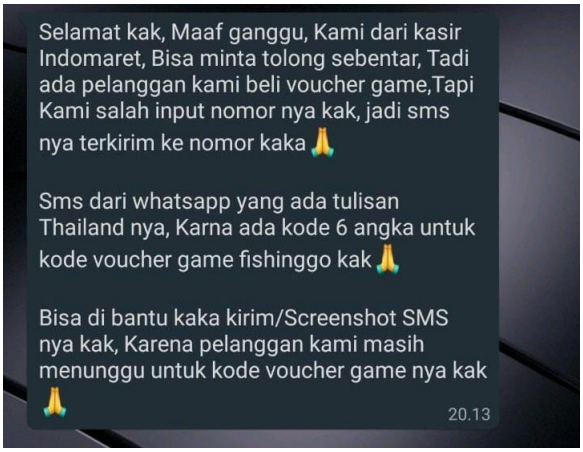
Dalam studi kasus kali ini, ialah bagaimana system pengguna dicuri oleh pelaku dengan menggunakan kode OTP, berikut adalah hasil dari diskusi yang telah dilakukan :

- Pertama, penipu akan menyadap global system for mobile communication (GSM) pada gawai, wifi maupun protokol sinyal SS7.
- Kedua, penipu mengirimkan software jahat seperti Malware atau trojan ke gadget korban. Kode OTP bisa dicuri karena korban menyundul software atau file yang memuat Malware.



Gambar.1. Penipuan OTP

- Ketiga, penipu melakukan phising atau mengelabui korban dengan berpura-pura menjadi petugas pusat informasi untuk menelpon calon korban dan mengambil data pribadinya. Dalam upaya phis- ing ini walaupun calon korban tidak memberikan kode OTP pun, korban masih bisa di retas yaitu dengan fitur pengalihan panggilan (call forward) yang sekaligus mengaktifkan sms forward. Oleh karena itu, pelaku menerima sms yang masuk ke ponsel korban, termasuk kode OTP. Penipu ma- suk ke akun whatsapp, go pay, tokopedia dan mencoba membeli barang dengan kartu kredit.



Gambar.2.Penipuan Kedok Pusat Informan

- Cara lainnya yaitu, dengan menyebarkan pesan ke banyak nomer secara acak atau sms blasting. Penipu mengambil data pribadi seperti nomer ponsel korban. Lalu melakukan sms blasting. pelaku mengelabui penerima pesan yang merespon.

Gambar.3.Penipuan SMS Blasting

Ini berarti bahwa sistem yang menggunakan kode OTP tidak menjamin keamanan secara spesifik selalu ada celah bagi hacker untuk meretasnya. Oleh karena itu, sangat disarankan adanya penambahan system keamanan yang lain yang sudah terbukti keamanannya. Untuk membatasi pihak ketiga yang tak ber- tanggung jawab.

V. KESIMPULAN

Berdasarkan hasil penelitian terhadap analisis system penipuan berbasis rekayasa sosial dengan kode otp, studi kasus peretasan media sosial. Disimpulkan bahwa :

1. Peretasan dengan kode OTP sangat rentan terkena penipuan atau hack dari pihak pihak ketiga yang tidak bertanggung jawab.
2. Berbagai modus hacker mampu memanipulasi pengguna dengan kalimat yang mempengaruhi psikologis pengguna.
3. Phising salah satu metode untuk mendapatkan kode otp dan data pribadi korban.

DAFTAR PUSTAKA

[1] CNN Indonesia, Writer.(2019). Mengenal OTP, Kode Rahasia yang Jadi Incaran Peretas. CNN Indonesia Teknologi.
[2] Kompas, Writer.(2020). Teknologi Makin Maju, Penipuan dengan Rekayasa Sosial Pun Berubah. KOMPAS.com.
[3] Course Net Writer.(2020). Perbedaan Hacking dan Ethical Hacking serta Jenis-Jenis Hacking. Course- net.com.
[4] Suryadi, Kurniawan.(2020).Phising: Pengertian, Cara Kerja dan Langkah Mengatasinya. Niagahoster Blog.