

Bahaya *Social Engineering* dalam Sosial Media

Sri Utami^{1*}, Dina Nur Afifah², Masduki Asbari³

^{1,2}Universitas Insan Pembangunan Indonesia, Indonesia

²Universitas Sebelas Maret, Surakarta, Indonesia

*Corresponding author: sriutami240814@gmail.com

Abstrak - Tujuan dari penelitian ini adalah untuk memaparkan bagaimana bahaya *Social Engineering* dalam ber sosial media. Dalam penelitian ini menggunakan pendekatan kualitatif dengan metode simak catat, yang bersumber dari kanal Youtube (Diskusi Bersama Sabrang MDP) yang berjudul “Filter dalam posting di sosmed”. Hasil telaah singkat dari proses menyimak kajian ini adalah tentang bagaimana cara kita agar bijak dan berhati-hati dalam memposting sesuatu di sosial media. Perilaku posting foto, video, atau tulisan yang berisikan informasi pribadi dapat menyebabkan pengguna berada dalam posisi yang berbahaya dan berpotensi hilangnya privasi pengguna. Banyak dari kejahatan dilakukan dengan tujuan untuk mendapatkan keuntungan. Pelaku mengambil foto dan informasi nomor telephone korban melalui sosial media dan mengedit foto korban menjadi foto vulgar untuk mengancam dan memeras korban. Kasus penyalahgunaan informasi disebabkan oleh kurangnya kesadaran untuk menjaga privasi informasi di media sosial. *Social engineering* merupakan salah satu teknik yang perlu diwaspadai dalam menjaga keamanan informasi. *Social Engineering* menyorot pada bagian terlemah pada sistem jaringan komputer, yaitu manusia. Teknik tersebut berusaha mengambil informasi pribadi dengan melakukan manipulasi psikologis melalui mekanisme interaksi sosial. Selain itu, dalam pelaksanaan *social engineering*, pelaku meminta langsung apa yang diinginkan.

Kata Kunci: *Social Engineering*, sosial media, keamanan informasi.

Abstract - The purpose of this research is to explain how the dangers of *Social Engineering* in using social media. In this study, a qualitative approach was used using the see note method, which was sourced from the Youtube channel (Diskusi Bersama Sabrang MDP) entitled "Filters in social media posts". The results of a brief review of the process of listening to this study are about how we can be wise and careful in posting something on social media. The behavior of posting photos, videos or writing that contains personal information can put users in a dangerous position and have the potential to lose user privacy. Many of the crimes are committed with the aim of gaining profit. The perpetrator took photos and telephone number information of the victim through social media and edited the victim's photo into a vulgar photo to threaten and blackmail the victim. Cases of misuse of information are caused by a lack of awareness to maintain the privacy of information on social media. *Social engineering* is a technique that needs to be watched out for in maintaining information security. *Social Engineering* focuses on the weakest part of the computer network system, namely humans. The technique seeks to retrieve personal information by carrying out psychological manipulation through social interaction mechanisms. In addition, in the implementation of *social engineering*, the perpetrator asks directly for what he wants.

Keywords: *Social Engineering*, social media, information security.

PENDAHULUAN

Pada awal tahun 2023 pengguna internet di Indonesia mencapai 212,9 juta. Angka tersebut mengalami pertumbuhan jika dibandingkan dengan periode yang sama di tahun lalu. Berdasarkan data

yang dirilis *We Are Social* menyebutkan total populasi Indonesia 276,4 juta, di mana 49,7 persen perempuan dan 50,3% pria pada Januari 2023. Jika dilihat dari pengguna internet, penduduk Indonesia yang berselancar di dunia maya itu ada 212,9 juta pengguna yang mana itu mengalami kenaikan 5,2% atau 10 juta dari 2022. Hal tersebut memicu semua platform media sosial akhirnya fokus untuk mengoptimalkan aplikasinya di perangkat mobile.

Sekarang ini banyak masyarakat yang berbisnis dari rumah dan menggunakan media sosial sebagai alat promosi. Media sosial sebagai alat promosi bisnis yang efektif karena dapat diakses oleh siapa saja, sehingga jaringan promosi bisa lebih luas. Media sosial menjadi bagian yang sangat diperlukan oleh pemasaran bagi banyak perusahaan dan merupakan salah cara terbaik untuk dapat menjangkau luasnya pasar ataupun pelanggan. Media sosial seperti Facebook, Twitter, Instagram, dan Youtube memiliki sejumlah manfaat sendiri bagi para pelaku usaha dibandingkan dengan menggunakan media konvensional sebagai media promosi.

Remaja dan anak-anak saat ini merupakan golongan masyarakat yang hidup di era digital (*digital native*). Sementara itu, generasi orang tua dari mereka saat ini masih cenderung menjadi penduduk pendatang digital (*digital immigrant*). Akibatnya, kesadaran akan potensi negatif yang akan mengancam anak-anak dan remaja tidak disadari dan diseriuisi oleh kalangan dewasa ataupun orang tua. Anak dan remaja dapat digambarkan sebagai *digital native*, merupakan kalangan serupa penduduk asli di dunia digital saat ini. Mereka lahir dan tumbuh di era digital yang menjadikan mereka memiliki cara berpikir, berbicara, dan bertindak berbeda dengan generasi sebelumnya yang diibaratkan sebagai *digital immigrant*.

Ketika sedang menggunakan media sosial, remaja memiliki sifat yang cukup terbuka karena adanya keinginan untuk tetap eksis dan viral dengan melakukan upload kegiatan yang sedang mereka lakukan dalam bentuk foto, video, maupun tulisan. Perilaku memposting seringkali berisikan informasi pribadi mereka tersebut dapat menyebabkan pengguna berada dalam posisi berbahaya dan berpotensi hilangnya privasi pengguna. Dalam beberapa kasus kriminal seputar penyalahgunaan informasi kerap kali terjadi di Indonesia. Banyak dari kasus tersebut dilakukan dengan tujuan untuk mendapatkan keuntungan. Pelaku mengambil foto dan informasi nomor seluler korban melalui sosial media dan mengedit foto korban menjadi foto berkonten negatif. Foto tersebut digunakan sebagai umpan untuk mengancam korban dan memeras korban. Kasus mengenai penyalahgunaan informasi tersebut disebabkan oleh kurangnya kesadaran akan pentingnya menjaga privasi informasi di media sosial. Orang tua mempunyai peranan yang sangat dalam mengarahkan penggunaan teknologi secara aman bagi keluarga dan masyarakat di sekitarnya.

Social engineering merupakan suatu kegiatan yang perlu diwaspadai dalam menjaga keamanan informasi. *Social engineering* sangat berfokus pada bagian terlemah pada sistem jaringan komputer, yaitu manusia. *Social engineering* merupakan salah satu teknik *hacking* yang paling mudah dilakukan karena dilakukan dengan cara mengeksploitasi kelemahan manusia seperti rasa takut, rasa percaya, dan rasa ingin menolong. Pada dasarnya teknik *social engineering* dibagi menjadi dua jenis, yaitu berbasis interaksi sosial dan berbasis interaksi komputer. Menurut eksperimen yang dilakukan oleh Bullée et al, peningkatan kesadaran tentang bahaya, karakteristik, dan penanggulangan yang terkait dengan *social engineering* terbukti memiliki efek positif yang signifikan dalam meminimalisir penyerangan.

METODE PENELITIAN

Dalam penelitian ini, peneliti menggunakan pendekatan kualitatif deskriptif. Menurut Bogdan dan Taylor (1992) dalam V. Wiratna Sujawerni (2020:19) menjelaskan bahwa penelitian kualitatif adalah penelitian yang menghasilkan data deskriptif, yakni ucapan atau tulisan dan perilaku orang-orang yang diamati. Pendekatan ini diharapkan dapat menghasilkan uraian yang mendalam tentang ucapan, tulisan, dan perilaku yang dapat diamati dari suatu individu, kelompok, masyarakat, dan organisasi tertentu dalam suatu keadaan konteks tertentu yang dikaji dari sudut pandang yang utuh, komprehensif, dan holistik.

Metode Penelitian Bahasa (2014), Muhammad (2010:23) mengemukakan bahwa di antara fenomena yang dapat menjadi objek penelitian kualitatif adalah fenomena atau peristiwa komunikasi

atau berbahasa karena peristiwa tersebut melibatkan tuturan, makna semantik tutur, orang yang bertutur, maksud yang bertutur, situasi tutur, peristiwa tutur, tindak tutur dan latar tutur. Metode pengumpulan data yang digunakan adalah metode simak catat karena sumber data yang peneliti diperoleh dengan menyimak video yang bersumber dari kanal Youtube (Diskusi Bersama Sabrang MDP) yang berjudul “Filter dalam posting di sosmed”. Sedangkan Objek penelitiannya adalah Kajian filosofis yang dilakukan Sabrang MDP. Instrumen penelitian yang dipakai oleh peneliti yaitu human interest, yang mana peneliti berperan sebagai instrumen utama.

HASIL DAN PEMBAHASAN

Hasil dari simak catat yang didapatkan dari kanal Youtube (Diskusi Bersama Sabrang MDP) yaitu, menceritakan tentang filter dalam posting di sosial media agar terhindar dari bahaya *social engineering*. Semakin canggih teknologi saat ini, semakin banyak kejahatan terjadi secara online. Akses mudah ke data seseorang akhir-akhir ini benar-benar pedang bermata dua, karena ada penjahat yang akan memburu kamu. Salah satu yang sering adalah tindakan *social engineering*.

Social engineering adalah jenis kejahatan online yang berupaya memnipulasi data pribadi atau rahasia. Penjahat ini dapat menyerang berbagai platform seperti email, media sosial, dll. Serangan semacam itu sering digunakan oleh pelaku untuk mencuri dan menghancurkan data pribadi korban untuk menipu atau mengancam data yang dimilikinya. Contoh yang mengejutkan banyak pengguna di jejaring sosial adalah fungsi “Add Yours” yang dulunya sangat populer di Instagram. Banyak orang yang akhirnya menyalahgunakan fitur ini dengan memberikan berbagai detail seperti umur, tanggal lahir, nama panggilan saat masih anak-anak, nama anak atau orang tuanya. Dampak dari tren tersebut kemudian dibarengi dengan meningkatnya kasus penipuan dengan menggunakan data yang mereka sebar melalui Instagram. Pelaku *Social engineering* adalah orang-orang yang mendapat untung dari psikologi korban biasa yang mudah dimanipulasi. Tindakan *cybercrime* ini sangat mempengaruhi keadaan emosi dan pikiran korban saat menerima umpan. Contoh lain adalah permintaan uang atau barang berharga lainnya, ketika pelaku menipu korban, yang langsung yakin dengan tipu muslihat pelaku. Tidak hanya serangan individu, serangan *social engineering* berpotensi menyerang seluruh perusahaan atau organisasi besar. Pesatnya perkembangan teknologi memaksa setiap perusahaan untuk memperkuat sistem keamanannya agar tidak ada celah untuk diretas.

Cara kerja *social engineering* biasanya pelaku melakukan perencanaan, riset terlebih dahulu dengan menggali dan meneliti target korbannya dengan hati-hati dan menyeluruh. Lalu pelaku akan mengembangkan pretext atau penampilan kata-kata yang akan digunakan untuk menipu korban, semakin meyakinkan kata-kata semakin mudah korban ditipu oleh trik *hacker*. Jika korban bereaksi terhadap serangan pelaku, peretas akan bertindak cepat untuk mengeksploitasi data dengan contoh meminta nomor akun, nomor ID, nomor selular, atau kata sandi jejaring sosial. Banyak *hacker* yang langsung memberikan link *phishing* kepada korban melalui pesan singkat untuk memudahkan akses mereka ke sistem perangkat korban. Yang terakhir peretas akan menginterupsi pesan atau komunikasi korban dalam sepersekian detik bisa menghilang. Hal ini membuat korban tidak mengetahui identitas peretas atau ancaman yang akan mereka terima selanjutnya.

Social Engineering memiliki beberapa kategori yang terbagi sesuai dengan metode yang digunakan pelaku, jenis jenis serangan *social engineering* yaitu pertama *scareware* (kejahatan dengan cara menakuti korban dengan *interface* peringatan atau tanda bahaya pada perangkat, yang kedua *tailgating* (kejahatan yang dilakukan secara langsung dengan menemui korban kemudian menggali berbagai informasi yang dibutuhkan pelaku, pelaku bisa saja menyamar menjadi siapa saja agar dapat melakukan aksinya dengan cara menipu korban), yang ketiga *pretexting* (kejahatan ini biasanya dilakukan di berbagai platform media sosial, salah satunya email, pelaku akan membuat akun rahasia dengan perusahaan terkenal yang menghancurkan kamu memasukkan data pribadi seperti kata sandi dan nomor ID), yang keempat *baiting* (teknik kejahatan dengan cara menjebak korban menggunakan umpan, biasanya terjadi ketika kita ingin mengunduh file di situs web dan kemudian berlanjut ke akses audio, folder, kontak, dll), yang kelima *phishing* (kejahatan yang dilakukan dengan cara membagikan suatu link atau tautan), yang keenam *quid pro quo* (taktik kejahatan yang menawarkan keuntungan atau jasa mereka).

Dengan adanya kasus-kasus yang sudah ada kita dapat mencegah agar terhindar dari bahaya *social engineering* yaitu dengan beberapa hal yaitu, jangan memberikan data pribadi di internet,

verifikasi akun agar akun yang kamu buat tetap aman, gunakan *two factor authentication* (lapisan ganda atau multifaktor) selalu gunakan sandi unik dan sulit ditebak untuk melindungi keamanan akun kamu, memasang antivirus, menggunakan filter spam email, menghindari klik link yang mencurigakan, berhati-hati dalam mendownload file.

KESIMPULAN

Perkembangan sosial media yang sangat cepat membuat kejahatan di dunia maya juga semakin banyak. Namun sayangnya, banyak orang yang belum sadar bahwa kejahatan dunia maya selalu mengincar calon korbannya. Sosial media merupakan faktor utama untuk melakukan kejahatan, hal itu dikarenakan saat ini banyak orang yang dengan mudahnya membagikan kehidupan pribadi mereka ke sosial media dan itu akan mengundang oknum yang menganggap bahwa hal tersebut merupakan *attack factoring* yang bisa dimanfaatkan. Banyak orang berfikir bahwa dengan sosial media bisa mendapatkan banyak teman, misalnya saja banyak notifikasi pertemanan, kita dengan mudahnya menerima agar bertambah *follower*. Orang-orang juga suka mendeskripsikan diri mereka di sosial media, misal memberi tahu sekolah, hobi, bahkan nomor telepon yang mereka cantumkan, mereka juga sering mengunggah aktivitas sehari-hari di sosial media. Hal yang tanpa disadari membentuk pola dan memiliki dampak besar untuk orang lain melakukan kejahatan. Jangan membagikan data pribadi dan penting di sosial media, hal tersebut justru akan berdampak buruk. Jangan mudah percayasi siapapun di dunia *cyber*. *Zero trust*. Karena kita tidak tahu orang-orang yang kita *follow* di sosial media itu mempunyai sisi negatif atau tidak, jadi harus *be aware*. Sementara itu tercatat ada 10-15 kasus *cyber crime* dalam setiap detiknya. Terlebih jika itu terjadi pada diri sendiri dan pelaku mencuri data atau aset penting untuk disalahgunakan. Hal ini berkaitan dengan pesan yang ada dalam video youtube (Diskusi Bersama Sabrang MDP) yang berjudul “Filter dalam posting di sosmed”, jadi postinglah apa yang kamu percayai dan apa yang kamu pahami. Mari bijak dalam bersosial media agar selalu terhindar dari hal-hal yang merugikan diri sendiri atau orang lain.

DAFTAR PUSTAKA

Asbari, M. (2015). *Fokus Satu Hebat*. Penerbit Dapur Buku.

Asbari, M., & Prasetya, A. B. (2021). Managerial Coaching: Rahasia Membangun Kinerja, Komitmen Tim dan Modal Psikologis Guru. *Edumaspul: Jurnal Pendidikan*, 5(1), 490-506 <https://doi.org/10.33487/edumaspul.v5i1.1248>

Asbari, M., Purwanto, A., & Novitasari, D. (2022). Diskursus Relasi Pengaruh Modal Psikologis terhadap Inovasi Guru. *Jurnal Pendidikan Transformatif*, 1(1), 1320. <https://doi.org/10.9000/jupetra.v1i1.3>

Asbari, M., Purwanto, A., & Novitasari, D. (2022). Kepuasan Kerja Guru: Diantara Kepemimpinan Transformasional dan Transaksional. *Jurnal Pendidikan Transformatif*, 1(1), 12 <https://doi.org/10.9000/jupetra.v1i1.2>

Aulia, T. N., & Asbari, M. (2023). Bahaya Digital Fatigue pada Kesehatan Mental: Analisis Singkat Perspektif Rhenald Kasali. *Literaksi: Jurnal Manajemen Pendidikan*, 1(01), 30-33.

Azhari, D. W., & Putri, W. F. (2023). Urgensi Moralitas Generasi Bangsa: Sebuah Esai. *Literaksi: Jurnal Manajemen Pendidikan*, 1(02), 7-11.

Azmi, A. F., & Asbari, M. (2022). Kenali Diri Agar Bahagia: Kajian Filosofis Fahrudin Faiz. *Jurnal Pendidikan Transformatif*, 2(1), 1-5. <https://doi.org/10.9000/jupetra.v2i1.9>

Baihaqi, M. F., & Asbari, M. (2022). Relakanlah untuk Sakit Sebentar: Sebuah Kajian Filsafat Singkat. *Jurnal Pendidikan Transformatif*, 2(1), 30-34. <https://doi.org/10.9000/jupetra.v2i1.41>

- Casika, A., Agniya, A. N., Hermawan, M. B., & Asbari, M. (2023). Pygmalion Effect: Dampak Kepercayaan terhadap Kinerja. *Literaksi: Jurnal Manajemen Pendidikan*, 1(01), 39-44.
- Casika, A., Lidia, A., & Asbari, M. (2023). Pendidikan Karakter dan Dekadensi Moral Kaum Milenial. *Literaksi: Jurnal Manajemen Pendidikan*, 1(01), 13-19.
- Chidir, G., Asbari, M., Purwanto, A., & Asbari, D. A. F. (2022). Pengaruh Learning dan Coaching Individu terhadap Kinerja Guru: Sebuah Telaah Singkat. *Jurnal Pendidikan Transformatif*, 1(1), 21–25. <https://doi.org/10.9000/jupetra.v1i1.4>
- Febriani, R., Asbari, M., & Yani, A. (2023). Resensi Buku: Berani Berubah untuk Hidup Lebih Baik. *Literaksi: Jurnal Manajemen Pendidikan*, 1(01), 1-6.
- Karima, R., Octavia, L. G. V., & Fahmi, K. (2023). Lunturnya Moralitas Pelajar Indonesia?. *Literaksi: Jurnal Manajemen Pendidikan*, 1(02), 17-20.
- Kurniawan, A., Daeli, S. I., Asbari, M., & Santoso, G. (2023). Krisis Moral Remaja di Era Digital. *Literaksi: Jurnal Manajemen Pendidikan*, 1(02), 21-25.
- Oliver, A., (2023). Social Engineering: Definisi, Jenis Serangan, dan Cara Mencegah <https://glints.com/id/lowongan/social-engineering/>
- Rahmawati, W., Asbari, M., & Cahyono, Y. (2023). Nilai Moral dan Etika: Perspektif Emile Durkheim. *Literaksi: Jurnal Manajemen Pendidikan*, 1(02), 12-16.
- Rusdi, A. (2016). Syukur dalam psikologi islam dan konstruksi alat ukurnya. *Jurnal Ilmiah Penelitian Psikologi: Kajian Empiris & Non-Empiris*, 2(2), 37-54.
- Sabrang, MDP. (2023). Filter dalam posting di sosmed. Channel youtube Sabrang MDP. <https://youtu.be/f64dlOFE-DU>
- SURYANINGRUM, F., (2022). WASPADAI SOCIAL ENGINEERING! PENGERTIAN & CARA MENCEGAHNYA <https://AKSARADATA.ID/BLOG/SOCIAL-ENGINEERING-ADALAH/>
- Tsoraya, N. D., Asbari, M., & Pratiwi, A. (2023). Revolusi Digital: Meningkatkan Relasi, Mengurangi Intensi. *Literaksi: Jurnal Manajemen Pendidikan*, 1(01), 34-38.
- Tsoraya, N. D., Khasanah, I. A., Asbari, M., & Purwanto, A. (2023). Pentingnya Pendidikan Karakter Terhadap Moralitas Pelajar di Lingkungan Masyarakat Era Digital. *Literaksi: Jurnal Manajemen Pendidikan*, 1(01), 7-12.
- Wijayanti, N. N., (2021). Social Engineering: Kejahatan Online yang Mungkin Tidak Anda Sadari. <https://www.niagahoster.co.id/blog/social-engineering-adalah/>
- Zeva, S., Rizqiana, I., Novitasari, D., & Radita, F. R. (2023). Moralitas Generasi Z di Media Sosial: Sebuah Esai. *Literaksi: Jurnal Manajemen Pendidikan*, 1(02), 1-6.