BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam dua dekade terakhir, kemajuan pesat media sosial telah menjadi sorotan. Setiap tahun, platform media sosial baru bermunculan dan jumlah penggunanya melebihi perkiraan. Di masa lalu, informasi hanya mengalir dari media massa konvensional seperti koran dan televisi, tetapi sekarang setiap pengguna media sosial dapat menjadi sumber informasi. Misalnya, ketika ada kecelakaan, dulu kita harus menunggu laporan resmi dari media, namun sekarang informasi tersebut dapat tersebar hanya dalam hitungan detik karena ada yang mengunggahnya ke media sosial. Pengguna media sosial di Indonesia juga terus bertambah setiap tahunnya, menunjukkan pengaruh besar perkembangan media sosial di negara ini.[1]

Kejahatan *cyber* merupakan salah satu jenis kejahatan yang menggunakan teknologi komputer dan jaringan internet. *Social engineering* merupakan salah satu jenis kejahatan *cyber* yaitu penipuan atau pembajakan melalui dunia maya. Hadnagy dalam bukunya yang berjudul "Social Engineering The Art of Human Hacking" mengatakan bahwa *social engineering* merupakan taktik untuk menjadi aktor yang baik, dan cara untuk mendapatkan sesuatu yang dibutuhkan secara gratis.[2] *Social engineering* juga merupakan taktik memanipulasi, memengaruhi, atau menipu korban untuk mendapatkan kendali atas sistem komputer, atau untuk mencuri informasi pribadi bahkan keuangan. Pelaku *social engineering* menggunakan teknik *social engineering* untuk menyembunyikan identitas dan meniru identitas individu tepercaya. Salah satu bahaya dari serangan *social engineering* adalah penampilannya yang tidak berbahaya sehingga targetnya (yaitu seseorang dan bukan sasaran serangan) tidak menyadari bahwa mereka telah menjadi korban. Tujuan praktik *social engineering* adalah untuk memengaruhi, memanipulasi, menipu pengguna lain agar percaya bahwa pelaku

---

[1] Antonius Mbukut, "Media Sosial dan Orientasi Diri Generasi Muda IndonesiaDitinjau dari Pemikiran Yuval Noah Harari", *Jurnal Filsafat Indonesia*, 7:1, (Universitas Pendidikan Ganesha: 30 April 2024), https://doi.org/10.23887/jfi.v7i1.67571, diakses 10 Juni 2024.

[2] Christopher Hadnagy, *Social Engineering: The Art of Human Hacking*, (Canada: Wiley Publishing, Inc., 2011), hlm. 9.

adalah pemilik akun atau untuk menipu korban secara finansial. *Social engineering* pada media sosial Facebook kerapkali terjadi kepada pengguna Facebook hanya mereka tidak menyadari hal itu.

Aplikasi media sosial Facebook didirikan pada tahun 2004 oleh Mark Zuckerberg dan rekan-rekannya di Harvard University. Facebook memungkinkan pengguna untuk terhubung dengan teman, keluarga, dan komunitas mereka secara *online*. *Platform* ini menyediakan berbagai fitur, termasuk berbagi status, foto, video, dan konten lainnya, serta berinteraksi melalui komentar dan berbagai reaksi lainnya. Facebook telah menjadi juara media sosial terpopuler di dunia selama beberapa tahun. Pada tahun 2023 Facebook masih menjadi aplikasi media sosial yang paling populer, dengan pengguna aktif sebanyak 2,958 miliar.[3]

Di Indonesia, Facebook telah menjadi salah satu *platform* media sosial yang paling populer, dengan pengguna beragam dari berbagai latar belakang usia, profesi, dan kepentingan. Indonesia adalah negara yang menempati peringkat ketiga dengan pengguna Facebook terbanyak setelah India dan Amerika Serikat.[4] Berdasarkan data Napoleon Cat, pengguna Facebook di Indonesia Januari 2024 terdapat 173,7 Juta pengguna, yang mencakup 61,7% dari seluruh penduduk Indonesia. Sebagian besar pengguna Facebook di Indonesia tercatat berasal dari kisaran usia generasi Z. Pengguna Facebook yang usianya 18-24 tahun mencapai 46,7 juta, atau 26,9% dari total pengguna. Ada juga sekitar 66 juta pengguna Facebook dari kelompok usia 25-34 tahun (38%). Posisinya diikuti kelompok usia 35-44 tahun (36,3 juta pengguna atau 20,9%), 45-54 tahun (15,5 juta pengguna atau 8,9%), dan 55-64 tahun (5,3 juta pengguna atau 3,1%). Pengguna paling sedikit dari kelompok usia 65 tahun ke atas, yakni 3,9 juta pengguna (2,2%). Mayoritas pengguna Facebook di Indonesia adalah laki-laki dengan proporsi 53,2%, sedangkan perempuan 46,8%.[5]

---

[3] Agnes Z. Yonatan, "7 Media Sosial Paling Populer 2023", dalam *Goodstats*, 12 Juli 2023, https://data.goodstats.id/statistic/agneszefanyayonatan/7-media-sosial-paling-populer-2023-VXb0M, diakses pada 20 November 2023.

[4] Statista, "Leading countries based on Facebook audience size as of January 2023", Desember 2023. https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-Facebook-users/, diakses pada 20 November 2023

[5] NapeleonCat, "Facebook users in Indonesia January 2024", https://napoleoncat.com/stats/Facebook-users-in-indonesia/2024/01/, diakses pada 20 November 2023.

Namun, Facebook juga telah menghadapi banyak keluhan dan kontroversi. Beberapa keluhan yang umum dilaporkan oleh pengguna Facebook termasuk privasi, keamanan, dan penyalahgunaan data. Salah satu kasus nyata *social engineering* yang terjadi di Facebook adalah kasus dimana pelaku *cyber* menggunakan teknik *phishing* untuk mencuri informasi pengguna. Berikut adalah contoh skenario yang mungkin terjadi: *Pertama*, penipu menciptakan pesan atau komentar palsu yang menyerupai Facebook, yang berisi tautan ke halaman *login* palsu. Pesan ini dikirim melalui pesan langsung, komentar di postingan, atau bahkan melalui grup atau halaman Facebook palsu, cara ini disebut dengan *phising. Kedua*, mengirim tautan ke halaman palsu, tautan yang disediakan dalam pesan atau komentar tersebut mengarahkan pengguna ke halaman web palsu yang menyerupai halaman login resmi Facebook. Halaman ini mungkin memiliki URL yang mirip dengan Facebook dan seringkali terlihat meyakinkan. *Ketiga*, memasukkan informasi *login*, pengguna yang terpedaya mungkin diminta untuk memasukkan nama pengguna dan kata sandi mereka ke dalam halaman *login* palsu tersebut. Informasi ini kemudian disimpan oleh pelaku untuk digunakan dalam tindakan penipuan selanjutnya. *Keempat,* akses ke akun, setelah mendapatkan informasi *login* pengguna, pelaku dapat mengakses akun Facebook korban. Mereka kemudian dapat menggunakan akun tersebut untuk melakukan berbagai tindakan penipuan, seperti mengirim pesan *spam* kepada teman-teman pengguna, memposting konten yang merugikan, atau bahkan mencuri informasi pribadi lainnya. Kasus-kasus seperti ini terjadi secara reguler di *platform*s media sosial, termasuk Facebook.[6]

Contoh kasus *social engineering* yang terjadi dalam Facebook. *Pertama,* skandal privasi data pertama bagi Facebook/Meta terjadi pada Maret 2018. Informasi menyebar ke seluruh dunia bahwa Cambridge Analytica, perusahaan pemasaran data di bawah SCL Elections Ltd., berhasil mengakses informasi pribadi tidak resmi dari 87 juta profil Facebook di Amerika Serikat.[7] *Kedua*,

[6]Alyssa Newcomb, "Garis waktu masalah privasi Facebook - dan tanggapannya", dalam *NBC News*, https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651, accessed by 20 November 2023.
[7] Novita Intan dan Nidia Zuraya, "Skandal Data Facebook-Cambridge Analytica Berakhir Damai", dalam *Republika*, https://ekonomi.republika.co.id/berita/rhb7st383/skandal-data-facebook-cambridge-analytica-berakhir-damai, diakses pada 20 November 2023.

dilansir dari *website Makasarmetro.com* bahwa pada 30 Juli 2019, Kepolisian Daerah Sulawesi Selatan menangkap dua orang pelaku peretasan akun Facebook yang dilakukan oleh siswa SMK di Sulawesi Selatan. JE, siswa SMK di Ogan Komering Ilir Sumatera Selatan, berperan sebagai pelaku utama, sedangkan Dicky, lulusan sekolah komputer di Palembang, Sumatera Selatan, berperan sebagai pembeli akun yang telah diretas. JE berhasil meretas akun grup Facebook lembaga info kejadian kota Makassar yang kemudian dijual ke Dicky sebesar Rp. 500.000. Dicky menjual kembali akun tersebut dengan harga 1,7 juta. JE menggunakan teknik tertentu untuk mengambil alih akun Facebook korban, I Wayan Wijaya, merupakan salah satu admin grup lembaga info kejadian Makassar Kota. JE berhasil meretas setidaknya lima akun pemegang admin grup Facebook, dengan sasarannya adalah akun yang memegang grup karena berisi banyak anggota yang dapat dengan mudah dijual. JE menggunakan jasa pihak ketiga, rekening bersama, untuk transaksi jual beli akun ilegal dengan Dicky.[8] *Ketiga*, dilansir dari *website Suara*.com kasus *social engineering* di Facebook terjadi ketika seorang pria tua di Sulawesi Selatan (Sulsel) menyamar sebagai santriwati di Facebook dan menipu seorang lelaki berusia 35 tahun di Kalimantan. Lelaki itu ingin menikah dan mengirim uang Rp 50 juta sebagai mahar, tetapi sosok asli santriwati cantik ternyata pria tua yang berumur 53 tahun. Korban melaporkan kasus tersebut ke polisi dan pelaku ditangkap. Kasus ini menunjukkan bahwa Facebook adalah media sosial yang rentan terjadinya kasus *social engineering*, tidak hanya mengenai keamanan data pribadi melainkan pelaku juga dengan leluasa memperdaya psikologi seseorang.[9]

Selain kasus *social engineering* yang terjadi di daerah lain, ada beberapa kasus *social engineering* yang juga dialami oleh mahasiswa Prodi Filsafat IFTK Ledalero Konvik SVD. Berdasarkan data kuesioner yang disebar kepada mahasiswa, terdapat beberapa kasus *social engineering* yang pernah dialami oleh mahasiswa IFTK antara lain: banyak mahasiswa yang pernah menerima pesan

[8] Haider, "Polda Sulsel Tangkap Siswa SMK Pembobol Akun Facebook Demi Uang Jutaan Rupiah", dalam *Makasarmetro.com*, https://makassarmetro.com/2019/07/31/polda-sulsel-tangkap-siswa-smk-pembobol-akun-Facebook-demi-uang-jutaan-rupiah, diakses pada 21 November 2023.
[9] Rinaldi Aban, "Pria Tua di Sulsel Nyamar Jadi Santriwati, Korban Tertipu dan Kehilangan Uang Rp 50 Juta", dalam *Suara.com*, https://www.suara.com/video/2023/09/24/161500/pria-tua-di-sulsel-nyamar-jadi-santriwati-korban-tertipu-dan-kehilangan-uang-rp-50-juta, diakses pada 21 November 2023.

yang berisikan tautan yang tidak dikenali dan banyak juga yang mengklik tautan tersebut. Hal ini mungkin tidak berbahaya tetapi juga bisa berbahaya, karena tautan yang dikirim bisa saja menjadi instrumen atau jalan bagi para pelaku untuk masuk ke dalam akun pengguna lain. Selain itu, hampir semua juga merasa bahwa privasi akun mereka terganggu atau tidak aman saat menggunakan Facebook, hal ini disebabkan banyak kasus yang terjadi bahwa para pengguna Facebook sering kena *hack* ataupun ditipu melalui Facebook. Hampir semua mahsiswa yang menggunakan Facebook juga pernah menjadi korban dari *social engineering*, dan pernah mendapat pesan dari orang yang tak dikenal dengan modus menawarkan bantuan uang tunai; Bahkan ada yang menyamar menggunakan nama akun mereka dan meminta-minta pulsa kepada orang lain yang tak dikenal. Terlepas dari banyak yang pernah mengalami *social engineering* ada juga beberapa pengguna Facebook dari Prodi Filsafat IFTK Ledalero Konvik SVD yang mampu melindungi privasi akun mereka dari ancaman *social engineering* di dalam Facebook.

Melihat fenomena ini, penelitian ini bertujuan untuk memberikan pemahaman yang lebih baik tentang bahaya *social engineering* di Facebook serta mendorong upaya perlindungan diri dan kesadaran akan keamanan *digital* di kalangan pengguna, khususnya mahasiswa Prodi Filsafat IFTK Ledalero konvik SVD. Jika seseorang dengan sengaja mengakses atau membobol sistem keamanan akun Facebook orang lain tanpa izin pengguna maka akan mendapatkan tindak pidana dan dapat dihukum berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 mengenai Informasi dan Transaksi Elektronik dan pelakunya dapat diancam dengan: hukuman penjara paling lama 8 tahun atau denda paling banyak Rp800 juta. Dalam hal ini pelaku berpura-pura menjadi pemilik akun orang lain dan menggunakannya untuk memanipulasi dan melakukan penipuan. Selain itu pelaku juga menuliskan kalimat di kolom status dan menyebarkannya tanpa persetujuan pemilik akun maka tindakan ini dilarang dalam Pasal 32 ayat (1) UU ITE dan pelaku dapat dipidana penjara paling lama 8 tahun atau membayar denda maksimal 2 miliar. Berdasarkan uraian di atas, maka peneliti mengangkat fenomena *social engineering* ini untuk dianalisis lebih jauh dan peneliti

mengambil judul "***Social Engineering* dalam Facebook Terhadap Mahasiswa Prodi Filsafat Institut Filsafat dan Teknologi Kreatif Ledalero (Studi Kasus: Konvik SVD)**" .

1.2. Rumusan Masalah

Bagaimana fenomena *social engineering* dalam Facebook terhadap Mahasiswa Prodi Filsafat IFTK Ledalero terlebih dalam Konvik SVD?

1.3. Tujuan Penelitian

Adapun yang menjadi tujuan penelitian dalam skripsi ini adalah untuk menganalisis fenomena *social engineering* tersebut terhadap mahasiswa IFTK Ledalero di media sosial Facebook.

1.4. Manfaat Penelitian

Adapun manfaat dari penelitian ini sebagai berikut:

1. Memberikan pemahaman yang lebih mendalam tentang fenomena *social engineering*, khususnya di media sosial seperti Facebook. Ini penting karena semakin banyak orang yang menggunakan media sosial Facebook, semakin penting pula untuk memahami risiko seperti *social engineering*.
2. Membantu mahasiswa Institut Filsafat dan Teknologi Kreatif Ledalero untuk lebih waspada terhadap ancaman *social engineering* sehingga dengan pengetahuan ini, mereka bisa lebih berhati-hati dalam berinteraksi di media sosial.
3. Menambah literatur dan pengetahuan tentang *social engineering*, khususnya dalam konteks Indonesia dan terlebih khusus lagi bagi mahasiswa IFTK Ledalero. Ini bisa menjadi referensi untuk penelitian selanjutnya.

1.5. Sistematika Penulisan

Pada bagian ini penulis akan merunutkan secara garis besar tentang sistematika penelitian dalam karya ilmiah ini dalam empat bab utama, yaitu akan dijelaskan sebagai berikut:

Bab I merupakan bagian pendahuluan. Bagian ini terdiri atas latar belakang penelitian, rumusan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, dan sistematika penelitian.

Bab II merupakan bagian landasan teoretis dan kajian pustaka dari penelitian terdahulu yang relevan. Bagian ini akan dideskripsikan tentang *social engineering*; arti, tipe-tipe serangan *social engineering*, sistematika serangan *social engineering*, karakteristik *social engineering*, dan faktor penyebab serangan *social engineering*. Facebook; definisi dan sejarah, fungsi tujuan dan manfaat (akan dijelaskan dalam satu bagian), serta keuntungan dan kerugian menggunakan Facebook. *Social engineering* yang terjadi dalam Facebook beserta contoh kasusnya. Penelitian terdahulu yang relevan dengan judul penelitian ini sebagai berikut; Abdullah Algarni (2019), Tommy Gunawan (2019), Edwin Donald Frauenstein (2020), Abdul Shareef Phallivalappi et al (2021), Nurul Hidayat et al (2023), Huong Ti Ngoc Ho et al, (2024).

Bab III merupakan bagian metode penelitian. Di bagian ini akan dideskripsikan mengenai metode penelitian yang digunakan dalam penulisan.

Bab IV merupakan bagian hasil dan pembahasan. Pada bagian ini akan dipaparkan hasil dan pembahasan mengenai fenomena *social engineering* pada media sosial Facebook terhadap mahasiswa IFTK Ledalero.

Bab V merupakan bagian penutup. Bagian ini berisikan kesimpulan dan saran yang berkaitan dengan pembahasan yang telah dideskripsikan pada bab-bab sebelumnya.