BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Teknologi informasi telah berkembang pesat saat ini, dan membawa banyak perubahan di berbagai sektor, mulai dari politik, hukum, budaya, dan ekonomi. Namun selain memberi manfaat bagi banyak orang. Perkembangan teknologi informasi saat ini juga menyebabkan munculnya berbagai bentuk-bentuk aktivitas kriminal baru atau yang lebih dikenal dengan istilah *cybercrime*/kejahatan dunia maya melalui internet. *Cybercrime* mengacu pada pelanggaran ketika penjahat memanfaatkan jaringan komputer, internet, dan menyalahgunakan teknologi digital sebagai sarana untuk melakukan kejahatan (Putra et al., 2023).

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mengungkapkan bahwa jumlah pengguna internet di Indonesia pada tahun 2024 telah mencapai 221 juta jiwa. Jumlah pengguna *internet* yang meningkat ini tentunya akan menyebabkan ancaman terhadap privasi yang dapat mengancam data pribadi pengguna (Pertahanan et al., n.d.). Perkembangan jumlah pengguna internet yang terjadi saat ini juga telah memberikan banyak kemudahan bagi masyarakat dalam berinteraksi, serta mengakses berbagai macam *platform* digital. Mulai dari *platform* pendidikan, hiburan seperti *game,* menonton film atau *streaming,* transaksi keuangan, hingga aktivitas sehari-hari seperti belanja *online*. Semua itu bisa dilakukan dengan mudah berkat perkembangan teknologi yang terjadi saat ini (Fata,

2021).

Seiring dengan perkembangan teknologi, *platform-platform* aplikasi perangkat lunak maupun *website* telah menjadi bagian penting dalam kehidupan sehari-hari masyarakat. *Google Play Store* dan *App Store* telah menyediakan puluhan bahkan ratusan ribu aplikasi yang dapat diunduh ke perangkat *mobile* baik berbasis *Android* maupun *iOS*. Salah satu contohnya adalah *platform* aplikasi *e-commerce* dengan jumlah ulasan pengguna terbanyak, yaitu *Shopee, Tokopedia*, *Lazada*, *Zalora*, *Bukalapa*k, dan lain sebagainya. *Platform-platform* tersebut menyediakan layanan bagi para pengguna untuk membeli dan menjual berbagai produk maupun jasa secara *online* (Andika et al., n.d.).

Secara umum, *platform e-commerce* dapat dimanfaatkan sebagai sarana untuk melakukan transaksi jual beli produk maupun jasa (Yusuf et al., 2022). Hasil survei yang dilakukan oleh *We Are Social* pada bulan April 2021 telah mengukuhkan Indonesia sebagai negara tertinggi di dunia yang menggunakan layanan *e-commerce,* di mana hasil survei tersebut menunjukkan angka sebanyak 88,1% pengguna *internet* di Indonesia pernah melakukan transaksi atau berbelanja secara *online*. Selain itu, menurut laporan data.indonesia.id yang dilansir dari *statista market insight* mengenai data pengguna *e-commerce* yang ada di Indonesia, terhitung sejak tahun 2018, sudah ada 93,42 juta pengguna *e-commerce* aktif di Indonesia, dan jumlahnya diprediksi akan terus mengalami peningkatan hingga 244,67 juta pengguna pada tahun 2027.

Gambar 1.1
Data Jumlah Pengguna *E-Commerce* di Indonesia
(Sumber: dataindonesia.id)

Salah satu hal yang menjadi fokus utama dengan adanya perkembangan teknologi, meningkatnya jumlah pengguna *internet,* dan meningkatnya jumlah pengguna *e-commerce* di Indonesia adalah keamanan sistem informasi. Sistem informasi saat ini sering kali menjadi target serangan keamanan (*security attack*) yang beragam (Safitri et al., 2020). Menurut *Organization of European Community Development* (OECD), *cybercrime* mencakup semua bentuk akses yang tidak sah terhadap transmisi data dan informasi, sehingga perlu digarisbawahi terkait pentingnya melindungi sistem informasi di era saat ini.

Tindakan *cybercrime* ini terus mengalami peningkatan seiring dengan perkembangan teknologi digital, informasi, dan komunikasi yang terjadi saat ini (Caniago & Sutabri, 2023). Salah satu jenis *cybercrime* yang marak terjadi saat ini adalah *social engineering* dengan teknik *phishing* (Gulo et al., 2020). *Cybercrime* juga seringkali berkaitan dengan kelemahan sistem keamanan jaringan atau *network security*. Karena informasi merupakan aset kunci untuk mencapai kesuksesan dalam implementasi keamanan jaringan atau *network security*

(Hidayah, 2020).

Social engineering merupakan salah satu jenis tindakan *cybercrime* dengan teknik manipulasi dan memanfaatkan kesalahan manusia untuk mendapatkan data-data pribadi. Serangan ini mencakup penipuan dan pencurian data yang bersifat pribadi/privasi (Wahyuni et al., 2022). Komponen terlemah dari sistem keamanan adalah manusia, karena pelaku akan melakukan berbagai cara agar dapat memperoleh informasi rahasia dari teknik manipulasi terhadap seseorang hingga dapat memberikan akses masuk ke dalam sistem dengan cara yang ilegal (Yanti et al., 2017).

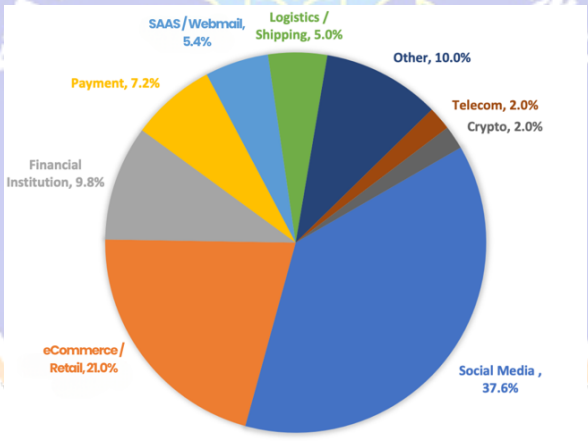
Salah satu dari sekian banyaknya jenis *cybercrime* yang paling cepat berkembang di *internet* adalah *Password Harvesting Fishing* (*Phishing*). *Phishing* merupakan salah satu jenis kejahatan siber yang bertujuan untuk mencuri data pribadi pengguna seperti *username* dan *password* secara ilegal (Putra et al., 2023). *Password Harvesting Fishing* (*Phishing*) merupakan sebuah aktivitas penipuan yang sering kali memanfaatkan *e-mail, link* atau situs web palsu untuk mengelabui pengguna agar memungkinkan pelaku memperoleh informasi atau data pribadi pengguna (Irawan, 2020).

Berdasarkan data terbaru dari *Phishing Activity Trends Report* yang dilansir dari *Anti-Phishing Working Group* (APWG) pada kuartal kedua tahun per tahun 2024, jumlah serangan unik pada situs *web phishing* yang terdeteksi telah mencapai 877,536 serangan yang mengincar berbagai sektor industri mulai dari *e-commerce*/retail, sosial media, *payment*, institusi finansial, dan lain sebagainya. Kaspersky juga mengungkapkan, pada awal 2024 praktik *phising* meningkat 40% dibandingkan dengan kuartal awal 2023. *Phising* sekarang juga banyak metode dan

jenisnya, mulai dari *voice phising, email phising, web phishing*, hingga QR *phising*. *Phising* memanfaatkan korban yang awam terhadap teknologi, dan baru-baru ini semakin gencar dilakukan melalui media sosial dan *e-commerce*.

	April	May	June
Number of unique phishing Web sites (attacks) detected	318,651	292,428	266,457
Unique phishing email campaigns	31,005	33,874	31,173
Number of brands targeted by phishing campaigns	324	320	301

Gambar 1.2
Jumlah Serangan Phishing Q2 2024
(Sumber: apwg.org)



Gambar 1.3
Jumlah Serangan *Phishing E-Commerce* Q2 2024
(Sumber: apwg.org)

Kasus *phishing* di Indonesia semakin marak terjadi pada *platform e-commerce* seperti *Shopee, Tokopedia*, *Lazada*, *Zalora*, *Bukalapa*k, dan lain sebagainya. Salah satu contoh dari banyaknya kasus *phishing* yang terjadi pada *platform e-commerce* adalah kasus yang menimpa pengguna *Zalora* pada tahun 2020, ketika pengguna layanan *e-commerce Zalora* tersebut menjadi korban

kejahatan *phishing*. Modus yang digunakan pelaku dimulai dengan panggilan telepon, di mana pelaku memberi tahu korban bahwa telah memenangkan hadiah. Setelah itu, pelaku mengirimkan link dan meminta korban untuk memasukkan kode *One-Time Password* (OTP) yang telah dikirim (Dokubani, 2020).

Selain itu, *phishing* juga dapat diartikan sebagai tindakan yang ditujukan untuk mendapatkan informasi pribadi yang bersifat rahasia dengan mengirimkan pesan palsu kepada pengguna melalui sarana komunikasi elektronik seperti *whatsapp*, telepon, *email*, dan lain sebagainya. Kegiatan penipuan ini dapat berupa pesan *whatsapp* yang seolah-olah berasal dari sebuah perusahaan maupun instansi resmi dan terpercaya dengan tujuan untuk mendapatkan informasi pribadi pengguna seperti *username, password, personal identification number (PIN)*, nomor rekening dan lain sebagainya. Oleh karena itu, melindungi sistem dari berbagai macam ancaman yang dapat membahayakan keamanan data dan informasi sangatlah penting untuk dilakukan (Herlambang et al., 2020).

Sehingga banyak dampak ditimbulkan yang akan sangat merugikan jika si pelaku telah berhasil masuk ke dalam akun *platform e-commerce* pengguna. Pelaku dapat melakukan pencurian data dan identitas, karena banyak *platform e-commerce* yang menyimpan data-data sensitif seperti nomor telepon, alamat rumah, KTP, dan lain sebagainya. Selain itu, jika penggunanya memasukkan kartu kredit/debit online dalam *e-commercenya*, maka pelaku akan dapat melihat rincian kartu kredit, yang bisa menampilkan rincian nomor kartu, tanggal kadaluwarsa, dan CVVnya, yang dapat dimanfaatkan untuk melakukan Carding.

Sejumlah penelitian sebelumnya menunjukkan bahwa *phishing* dapat terjadi di media sosial dan *platform* digital lainnya. Namun, penelitian spesifik mengenai

keamanan *e-commerce* terhadap risiko penyalahgunaan oleh para pelaku *cybercrime* untuk melakukan serangan *phishing* ke pengguna masih sangat terbatas. Penelitian yang dilakukan oleh (Fata, 2021) menguji keamanan informasi di *social media* menggunakan aplikasi *Social Engineering Toolkit* (SET), yang berhasil mereplikasi halaman *Facebook*. Penelitian ini menunjukkan bahwa *phishing* dapat terjadi di semua *platform social media*. Sedangkan penelitian yang dilakukan oleh (Puspitasari & Sutabri, 2023) fokus pada kajian literatur tentang *phishing* dan *cybercrime* pada *platform e-commerce* secara umum, khususnya *Shopee*, namun tidak sampai melakukan uji coba untuk melakukan teknik *phishing* tersebut. Selain itu, penelitian ini hanya meneliti satu *platform* saja.

Oleh karena itu, penelitian ini bertujuan untuk menganalisis keamanan *platform e-commerce* terhadap risiko penyalahgunaan oleh para pelaku *cybercrime* untuk melakukan serangan *social engineering* (*Phishing*) ke pengguna. Secara spesifik, penelitian ini akan menguji apakah situs *e-commerce* tersebut dapat direplikasi untuk menjebak pengguna agar memasukkan informasi pribadi mereka, seperti *username* dan *password* saat proses *login*. Selain itu, penelitian ini juga akan dapat memberikan informasi yang berguna bagi para pengguna untuk memilih *platform e-commerce* yang lebih aman, terpercaya, dan terbebas dari risiko penyalahgunaan oleh para pelaku *cybercime*. Serta membantu pemilik maupun pelaku usaha *e-commerce* untuk mengidentifikasi kelemahan yang ada dalam sistem keamanan *platform e-commerce* mereka, sehingga mereka dapat dengan segera mengambil tindakan perbaikan.

Pengujian dalam penelitian ini akan dilakukan dengan metode *Action Research* menggunakan aplikasi *Social Engineering Toolkit (SET)* pada sistem

operasi *Kali Linux*. Di mana *kali linux* merupakan distribusi *Linux* berbasis *Debian* yang secara khusus dirancang untuk keperluan *digital forensics* dan *penetration testing*. *Kali Linux* dikenal sebagai salah satu alat utama di kalangan praktisi keamanan siber, *Kali Linux* dilengkapi dengan berbagai alat dan utilitas yang mendukung analisis keamanan jaringan, pengujian kerentanan, serta pemulihan data. Dilihat dalam hal kinerja, *Kali Linux* juga telah mendapatkan perhatian luas berkat efisiensinya dalam melaksanakan uji penetrasi keamanan, yang memungkinkan pengguna untuk mengidentifikasi dan mengeksploitasi kerentanan yang ada dalam suatu sistem dengan cepat dan efektif. (Hindami et al., 2024).

1.2 RUMUSAN MASALAH

Berdasarkan pemaparan latar belakang tersebut, maka dapat ditarik sebuah permasalahan yang akan dijadikan dasar dalam penelitian ini, diantaranya:

1. Bagaimana keamanan *platform e-commerce* di Indonesia terhadap risiko penyalahgunaan oleh para pelaku *cybercrime* untuk melakukan serangan *phishing* menggunakan aplikasi SET?
2. Bagaimana efektivitas (persentase keberhasilan) *Social Engineering Toolkit* (SET) dalam melakukan pengujian keamanan melalui simulasi serangan phishing?

1.3 TUJUAN PENELITIAN

Berdasarkan rumusan masalah yang telah diuraikan diatas, adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk menganalisis keamanan *platform e-commerce* di Indonesia terhadap risiko penyalahgunaan oleh pelaku *cybercrime* untuk melakukan serangan

Phishing.

2. Untuk mengetahui efektivitas (persentase tingkat keberhasilan) *Social Engineering Toolkit* (SET) dalam melakukan pengujian keamanan melalui simulasi serangan phishing.

1.4 BATASAN MASALAH PENELITIAN

Untuk memperjelas fokus penelitian, adapun batasan masalah yang peneliti terapkan dalam penelitian ini diantaranya:

1. Penelitian ini akan memilih *platform e-commerce* yang masih aktif dan yang sudah familiar atau populer di Indonesia untuk diuji keamanannya. Pemilihan *platform* didasarkan dengan mempertimbangkan jumlah pengguna dan jumlah pengunjung berdasarkan data dari pusat data dan sistem informasi RI.
2. Penelitian ini akan melakukan pengujian untuk mengetahui efektivitas dari segi persentase keberhasilan *Social Engineering Toolkit* (SET) dalam melakukan serangan *Social Engineering Toolkit* (SET) untuk menguji keamanan *platform e-commerce*. Namun penelitian ini hanya sebatas menguji apakah *Social Engineering Toolkit* dapat mereplikasi *platform-platform e-commerce* yang diuji sehingga berisiko dimanfaatkan oleh para pelaku *cybercrime* untuk melakukan serangan *phishing*.
3. Pengujian yang dilakukan dalam penelitian ini bersifat pribadi (peneliti bertindak sebagai penguji sekaligus korban). Peneliti tidak akan menyebarkan *link phishing* dari *platform e-commerce* yang telah direplikasi, karena tindakan tersebut termasuk dalam kategori kejahatan yang dilarang oleh undang-undang.

1.5 MANFAAT PENELITIAN

Berdasarkan penelitian yang dilakukan, adapun manfaat yang diharapkan dari penelitian terkait analisis keamanan *platform e-commerce* di Indonesia terhadap serangan *phishing* adalah sebagai berikut.

1. Manfaat Teoritis

Pengembagan ilmu pengetahuan tentang teori keamaan siber, penelitian ini akan memperluas literatur dalam bidang keamanan siber dengan menambah pemahaman baru mengenai kerentanan yang ada pada *platform e-commerce* di Indonesia terhadap serangan *phishing*. Hasil atau temuan dari penelitian ini nantinya dapat digunakan sebagai dasar atau acuan untuk pengembangan teori-teori baru atau penguatan teori yang sudah ada sebelumnya dalam konteks keamanan informasi dan perlindungan data pribadi pengguna.

2. Manfaat Praktis

   a. Bagi Peneliti

   Penelitian ini akan memperdalam serta memperluas pemahaman peneliti tentang keamanan siber, khususnya terkait dengan serangan *phishing* dan keamanan *platform e-commerce*. Hasil penelitian ini juga dapat menjadi referensi atau acuan bagi para peneliti berikutnya mengidentifikasi celah-celah keamanan baru terhadap serangan *phishing* pada *platform e-commerce*

   b. Bagi Para Pengguna *E-Commerce*

   Penelitian ini akan dapat meningkatkan kesadaran masyarakat akan pentingnya keamanan data pribadi dan risiko serangan *phishing*. Selain itu, hasil penelitian ini juga dapat memberikan informasi yang berguna bagi para pengguna atau masyarakat untuk memilih *platform e-comm*erce yang lebih

aman, terpercaya, dan terbebas dari risiko serangan *phishing*.

c. Bagi Para Pemilik atau Pelaku *E-Commerce*

Hasil dari penelitian ini dapat membantu pemilik maupun pelaku usaha *e-commerce* untuk mengidentifikasi kelemahan yang ada dalam sistem keamanan *platform e-commerce* mereka, sehingga mereka dapat dengan segera mengambil tindakan perbaikan. Dengan mengambil tindakan perbaikan dan meningkatkan keamanan sistem, pemilik maupun pelaku usaha e-*commerce* akan dapat mencegah terjadinya kebocoran data pribadi pengguna yang dapat berdampak buruk pada reputasi dan bisnis *e-commerce* mereka.