BAB II

PERKEMBANGAN KASUS KEJAHATAN *CYBER PHISHING* DI SINGAPURA 2018-2025

Kejahatan siber *phishing* telah berkembang menjadi ancaman siber transnasional yang semakin kompleks seiring dengan digitalisasi layanan keuangan global. Modus serangan ini menggunakan rekayasa sosial dan manipulasi psikologis untuk mendapatkan akses ilegal ke data pribadi dan finansial, sehingga menempatkan pengguna sebagai titik lemah dalam sistem keamanan digital. Fenomena *phishing* tidak hanya menimbulkan kerugian ekonomi bagi individu, tetapi juga mengancam integritas sistem keuangan dan kepercayaan publik terhadap transaksi digital. Oleh karena itu, isu ini menjadi fokus utama dalam diskursus keamanan siber internasional dan mendorong perlunya strategi perlindungan yang adaptif dan multidimensional.

Singapura merupakan negara sebagai pusat keuangan internasional di Asia Tenggara, telah membangun infrastruktur kebijakan keamanan siber untuk melindungi infrastruktur informasi penting melalui *Melalui Cyber Security Agency of Singapore* (CSA) dan *Cybersecurity Act* 2018. Walaupun demikian, pengalaman serangan *phishing* berskala besar di Singapura menunjukkan bahwa peraturan dan teknologi belum sepenuhnya mampu mengimbangi ancaman yang menargetkan perilaku digital masyarakat dan kerentanan psikologis masyarakat. Kondisi ini menunjukkan bahwa pertahanan siber bukan hanya masalah teknis saja, tetapi juga memerlukan kesiapan institusional, kemampuan masyarakat untuk

mengidentifikasi ancaman, dan mekanisme kerja sama antarnegara untuk membangun pertahanan.

Untuk memahami kompleksitas tantangan keamanan siber yang dihadapi oleh singapura dalam menghadapi serangan siber *phishing*, bab ini disusun untuk memberikan gambaran faktual mengenai dinamika ancaman *phishing* dan respons keamanan digital yang dibentuk di tingkat nasional maupun regional. Pembahasan dalam bab ini mencakup definisi dan karakteristik *phishing*, pola serangan berbasis rekayasa sosial, serta bentuk-bentuk kerentanan digital masyarakat yang digunakan oleh pelaku kejahatan siber. Selain itu, bab ini juga membahas peran *Cyber Security Agency of Singapore* (CSA) dalam meningkatkan literasi keamanan digital melalui kampanye kesadaran public yang bertujuan untuk meningkatkan kesiapsiagaan Singapura menghadapi ancaman *phishing*.

2.1. Pertahanan *Cyber Security* di Singapura dengan *Cyber Security Agency of Singapore* (CSA)

Cyber Security Agency of Singapore (CSA) adalah lembaga pemerintah nasional yang secara resmi dibentuk pada 1 April 2015 dan ditempatkan di bawah koordinasi Kantor Perdana Menteri Singapura untuk memimpin dan mengoordinasikan strategi nasional keamanan siber. Lembaga ini lahir sebagai respons terhadap meningkatnya ancaman siber yang kompleks di tengah transformasi digital negara Singapura. CSA berasal dari konsolidasi beberapa unit yang sebelumnya ada di berbagai lembaga, seperti *Singapore Infocomm Technology Security Authority* (SITSA) dan *Singapore Computer Emergency*

Response Team (SingCERT), yang kemudian digabungkan agar lebih terintegrasi dan efektif dalam menghadapi eskalasi ancaman siber di Singapura. Singapura berharap untuk membentuk lembaga tunggal yang memiliki otoritas, koordinasi, dan kemampuan teknis yang lebih terintegrasi dengan menggabungkan konsolidasi fungsi tersebut (CSA, 2015).

Pemerintah Singapura memberikan CSA mandat strategis yang luas sebagai otoritas utama di bidang keamanan siber. Fungsi utamanya mencakup perlindungan *Critical Information Infrastructure* (CII) yang terdiri atas sektor vital seperti energi, kesehatan, perbankan, transportasi, dan telekomunikasi. Selain itu, CSA juga ditugaskan untuk membangun literasi publik tentang keamanan digital, meningkatkan kemampuan sumber daya manusia profesional di bidang teknologi informasi, serta memperkuat kerja sama internasional dengan negara-negara mitra. Untuk memperjelas arah organisasinya, CSA menetapkan misi resmi yakni "*keeping our cyberspace safe and secure to underpin our national security, power a digital economy, and protect our digital way of life."* Visi lembaga ini adalah membangun ruang siber yang tepercaya dan tangguh agar Singapura mampu menangkap peluang dari dunia yang semakin terkoneksi. Nilai-nilai utama yang dijunjung adalah inklusivitas, profesionalisme, keberanian, dan komitmen, yang membentuk budaya kerja CSA dalam menghadapi tantangan global (CSA, 2021).

Selain berfungsi sebagai lembaga kebijakan, CSA juga berpartisipasi dalam operasi teknis yang bertujuan untuk memastikan keamanan ruang siber nasional. CSA bertugas melakukan pemantauan ancaman, mendeteksi serangan, serta mengoordinasikan respons insiden, khususnya yang menargetkan *Critical*

Information Infrastructure (CII). Tugas ini mencakup investigasi forensik digital, mitigasi, dan pemulihan pasca insiden. Untuk meningkatkan kesiapsiagaan, CSA secara rutin menyelenggarakan latihan keamanan siber, termasuk *Cybersecurity Exercise* (CyEx) yang melibatkan sektor publik dan swasta. Upaya ini turut diakui secara internasional, dengan Singapura menempati peringkat keempat dunia dalam *Global Cybersecurity Index* 2020 yang diterbitkan *oleh International Telecommunication Union* (ITU, 2021).

Di luar lingkup domestik, CSA aktif memperkuat kerja sama regional dan global untuk menghadapi ancaman lintas batas. Singapura melalui CSA berpartisipasi dalam forum seperti ASEAN *Ministerial Conference on Cybersecurity* (AMCC) dan ASEAN CERT *Incident Drill* (ACID), yang menjadi sarana koordinasi antarnegara di Asia Tenggara. Selain itu, CSA juga menjalin kemitraan strategis dengan sektor swasta, lembaga riset, dan universitas untuk mengembangkan solusi inovatif serta memperluas literasi digital masyarakat. Inisiatif tersebut memperkuat posisi Singapura sebagai pemimpin regional di bidang keamanan siber, sekaligus mendukung reputasinya sebagai pusat digital yang aman di Asia Tenggara.

2.1.2. Upaya Teknis CSA untuk Menangani Ancaman Kejahatan Siber *Phishing*

Upaya teknis yang dilakukan oleh CSA berfokus pada peningkatan kemampuan deteksi dini serta mitigasi ancaman *phishing* melalui sistem pemantauan nasional dan penerbitan *technical advisory*. Salah satu contohnya adalah *Joint Advisory on Technical Support Scams*, yang

diterbitkan oleh Kepolisian singapura pada Januari 2025, yang menjelaskan bahwa modus serangan *phishing* menggunakan *pop-up* palsu dan perangkat lunak jarak jauh. Selain itu, panduan tersebut menekankan langkah mitigasi teknis seperti, pembaruan kata sandi, penghentian akses aplikasi berbahaya, dan pelaporan kepada otoritas keamanan. Upaya tersebut menunjukkan bahwa CSA mengambil langkah teknis untuk menangani ancaman siber yang terus berkembang (Singapore Police Force, 2025).

CSA juga mengembangkan *Safe App Portal* yaitu sistem evaluasi keamanan aplikasi yang berfungsi untuk melacak izin akses berlebihan, ancaman *malware,* dan perilaku berbahaya pada aplikasi digital. Portal ini memungkinkan pengembang dan pengguna untuk dapat memverifikasi keamanan aplikasi sebelum digunakan secara luas. Inisiatif ini merupakan bagian dari strategi teknis CSA untuk memperkuat keamanan digital di sektor perbankan dan layanan daring yang rentan terhadap *phishing*. CSA menunjukkan strategi pencegahan dan adaptasi terhadap ancaman siber yang semakin kompleks dengan memfokuskan pada keamanan aplikasi mobile (CSA, 2025).

Selain itu, CSA memperluas strategi teknisnya dengan mengintegrasikan keamanan *cloud*, *artificial intelligence* (AI), dan *operational technology* (OT) ke dalam skema sertifikasi nasional yaitu *Cyber Essentials* dan *Cyber Trust*. Kebijakan ini dapat meningkatkan pengamanan terhadap serangan *phishing* yang memanfaatkan teknologi canggih dan mendorong penerapan control teknis seperti segmentasi

jaringan keamanan OT/IT, dan model tanggung jawab bersama (*shared responsibility* model) pada layanan digital. Langkah tersebut menunjukkan bahwa strategi CSA akan berubah dari sekedar melindungi sistem konvensional ke arah arsitektur keamanan yang komprehensif dan adaptif. Oleh karena itu, strategi teknis CSA memainkan peran penting dalam membangun ketahanan siber nasional yang proaktif terhadap eksploitasi digital lintas sektor .(Cyber Security Agency of Singapore, 2025)

2.2. Perkembangan Kasus Kejahatan *Cyber Phishing* yang Terjadi di Singapura 2018-2025

2.2.1. Kejahatan *Cyber Phishing*

Phishing adalah bentuk kejahatan siber dimana pelaku mengirimkan pesan palsu, biasanya melalui email atau SMS yang berisikan tautan ke situs web berbahaya. Tujuan utama dari *phishing* adalah mencuri informasi sensitif seperti kata sandi, data pribadi, atau bahkan menipu korban agar mentransfer uang. Serangan *phishing* sering kali dilakukan dengan menyamarkan pesan agar tampak berasal dari sumber resmi, sehingga korban tidak menyadari bahwa mereka sedang menjadi sasaran kejahatan siber (National Cyber Security Centre, 2018).

Phsihing umumnya dilakukan dengan memalsukan identitas pengirim serta memalsukan tampilan pesan agar terlihat resmi, seperti mengunakan logo, alamt email, atau halaman web atau situs yang menyerupai lembaga keuangan atau layanan online yang sah. Pelaku

kejahatan *phishing* selanjutnya meminta korban untuk mengklik tautan palsu atau mengisi formulir *online* yang informasi pribadi seperti nama pengguna, kata sandi, dan informasi keuangan. Dalam beberapa kasus, pesan tersebut juga mengandung lampiran berbahaya. Lampiran tersebut dapat menginstal perangkat lunak berbahaya pada perangkat korban sehingga memungkinkan akses tidak sah terhadap data pribadi. Banyak korban tidak menyadari bahwa mereka sedang menjadi target kejahatan siber karena serangan ini sangat efektif dengan meniru komunikasi resmi yang sering diterima pengguna (Kosinski, 2023).

Serangan *phishing* kini berkembang menjadi serangan yang lebih terarah seperti *whaling*, yang menargetkan pejabat tinggi atau eksekutif perusahaan dan *spear phishing* yang menyasar individu atau organisasi tertentu. Pelaku juga memanfaatkan berbagai media digital, seperti pesan singkat (*smishing*), panggilan suara (*vishing*), dan kode QR palsu (*quishing*), untuk memperluas jangkauan serangan. Perkembangan serangan *phishing* menunjukkan bahwa *phishing* menjadi ancaman yang kompleks dan sistematis terhadap keamanan informasi. Dampak dari *phishing* tidak hanya mencakup kerugian finansial, melainkan juga kebocoran data pribadi seseorang serta gangguan reputasi dan kepercayaan publik terhadap sistem digital saat ini (CISA, 2024).

2.2.2. Sejarah Kejahatan *Cyber Phishing* di Asia Tenggara dan Singapura

Cyber phishing menjadi salah satu bentuk kejahatan siber yang paling menonjol dalam dua dekade terakhir karena *phishing* memanfaatkan rekayasa sosial untuk melakukan penipuan agar korban memberikan informasi pribadi maupun finansial pribadi mereka. Praktik *phishing* ini pertama kali muncul pada era 1990-an secara global, namun kejahatan ini semakin meluas di Kawasan Asia Tenggara seiring meningkatnya penggunaan layanan digital yang ada di masyarakat. *Phishing* telah muncul di beberapa negara ASEAN sejak awal tahun 2000-an dan mencapai puncaknya selama pandemic COVID-19, Ketika banyak aktivitas masyarakat yang beralih ke *platform online*. Berdasarkan data menurut Laporan *Anti-Phishing Working Group* (APWG) pada kuartal I 2025, terjadi hampir 1 juta serangan *phishing*. Hal ini menunjukkan bahwa ancaman *phishing* terus meningkat dan mempengaruhi Kawasan Asia Tenggara (APWG, 2025). *Phishing* dimulai dengan tahap awal yaitu melalui email dan situs web palsu yang meniru layanan resmi untuk mengelabui korban.

Di Kawasan Asia Tenggara kejahatan *cyber phishing* mulai muncul pada awal tahun 2000-an Ketika penggunaan internet mulai meluas di berbagai negara ASEAN. Modus ini semakin beragam seiring kemajuan teknologi, dan sekarang mencakup pesan singkat, media sosial, dan skema penipuan investasi berbasis *daring*. Transformasi ini dipercepat oleh pandemi COVID-19 karena semakin banyak aktivitas masyarakat beralih

ke ranah digital, yang memberi pelaku kejahatan lebih banyak kesempatan. Hal ini menandai bahwa *phishing* di Asia Tenggara berkembang dari praktik penipuan sederhana menjadi ancaman siber yang lebih kompleks dan lintas negara (Asialink, 2024).

Sementara itu, di Singapura sejarah *phishing* sejalan dengan pertumbuhan pesat infrastruktur digital negara sejak awal 2000-an. Sebagai pusat keuangan dan teknologi di Asia Tenggara, Singapura sejak awal menjadi salah satu target utama dalam kejahtan *cyber phishing* karena tingginya ativitas perbankan dan transaksi *daring* yang terjadi di Singapura. Pada awalnya, modus *cyber phishing* melalui email menjadi lebih kompleks dengan penggunaan SMS, aplikasi perpesanan, dan platform media sosial. Pemerintah Singapura secara bertahap memperkuat strategi keamanan siber melalui pembentukan lembaga khusus, kampanye literasi digital, dan kolaborasi lintas lembaga. Oleh karena itu, sejarah *phishing* di Singapura menunjukkan dinamika antara kemajuan teknologi dan upaya negara untuk menekan risiko yang muncul (Octavia, 2025).

2.2.3. Dampak Kejahatan *Cyber Phishing* di Singapura

Kejahatan siber *phishing* yang terjadi di Singapura memiliki dampak yang sangat signifikan terhadap stabilitas ekonomi masyarakat digital negara Singapura yang semakin bergantung pada sistem *online. Phishing* menyebabkan kerugian finansial langsung yang signifikan karena pelaku dapat memperoleh akses ke akun pribadi dan melakukan transaksi ilegal dengan cepat. Teknik manipulatif yang membuat situs palsu terlihat

sangat mirip dengan situs resmi menyebabkan banyak korban kehilangan dana tabungan dan aset digital mereka. Situasi ini menimbulkan kekhawatiran ekonomi dan menurunkan kepercayaan masyarakat terhadap sistem keuangan digital, yang pada awalnya dianggap kuat dan aman (Loh et al., 2024).

Korban kejahatan *phishing* di Singapura juga mengalami dampak psikologis yang signifikan karena mereka tidak hanya kehilangan uang tetapi juga mengalami trauma sosial dan tekanan emosional. Banyak korban mengalami perasaan malu dan bersalah karena tertipu, bahkan hingga mereka kehilangan kepercayaan diri mereka sendiri dalam menghadapi dunia digital. Dampak jangka panjang yang umum terjadi adalah kecemasan dan takut untuk kembali menggunakan layanan *online*. Kondisi ini menunjukkan bahwa *phishing* bukan hanya menyerang aspek ekonomi, tetapi juga mengguncang stabilitas mental dan rasa aman individu dalam kehidupan modern yang serba digital (H. M. Buse et al., 2023).

Selain itu, dampak sosial dan kepercayaan publik akibat kejahatan *phishing* di Singapura menjadi persoalan serius yang berpengaruh pada hubungan antara masyarakat dan sistem digital. Jumlah serangan yang meningkat membuat banyak orang tidak lagi percaya pada platform *daring* seperti layanan keuangan, *e-commerce*, dan portal pemerintahan digital. Ketakutan akan penipuan mendorong sebagian masyarakat untuk menghindari aktivitas digital yang penting untuk kehidupan modern. Akibatnya, kejahatan *phishing* tidak hanya menyebabkan kerugian bagi

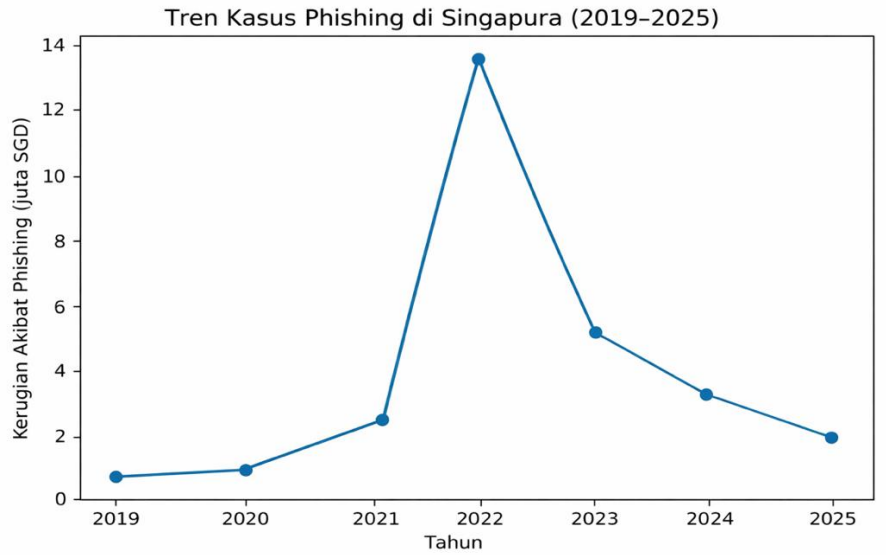
individu, tetapi juga merusak kepercayaan masyarakat dan reputasi Singapura sebagai negara yang unggul dalam keamanan (Ei & Soon, 2022).

2.2.4. Kasus Kejahatan *Cyber Phishing* yang terjadi di Singapura

Di era digital saat ini, layanan perbankan di Singapura semakin mengandalkan sistem *daring* dan *mobile banking* untuk memudahkan transaksi nasabah. Kemudahan layanan ini tentu sangat membawa manfaat yang besar, tetapi juga membuka peluang bagi pelaku kejahatan siber, terutama melalui *phishing*. *Phishing* adalah jenis penipuan yang memanfaatkan email, SMS, atau pesan instan palsu untuk menipu korban agar korban memberikan informasi pribadinya atau kredensial login. Fenomena ini menimbulkan risiko finansial yang besar bagi nasabah bank dan dapat merusak reputasi institusi keuangan. Menurut *Chambers Practice Guide on Cybersecurity* 2025, sektor perbankan menjadi target utama, dengan 63% dari seluruh upaya *phishing* menimpa institusi keuangan di Singapura (Jacob et al., 2025b).

Phishing sebagai salah satu bentuk kejahatan siber merupakan ancaman serius bagi keamanan digital di era transformasi teknologi. Modus ini umumnya dilakukan dengan cara menipu korban melalui email, pesan singkat, atau situs palsu agar secara tidak sadar memberikan informasi sensitif. Data yang dicuri dari praktik *phishing* dapat berupa identitas pribadi seperti nama, alamat, nomor rekening, kata sandi, maupun data finansial yang melekat pada akun perbankan. Dampaknya tidak hanya sebatas kerugian material akibat penipuan dan pencurian identitas, tetapi

juga berpotensi merusak kepercayaan publik terhadap lembaga perbankan sebagai pengelola data dan dana masyarakat. Hal ini menjadikan *phishing* bukan sekadar ancaman teknis, tetapi juga masalah kepercayaan yang berdampak langsung pada stabilitas sistem keuangan (Gupta et al., 2022)



Gambar 2. 1 *Tren Kasus Phishing di Singapura* (2019-2025)

Sumber: *Diolah oleh penulis (2025)*

Gambar 2.1. menunjukkan tren perkembangan kasus *phishing* di Singapura dalam periode 2019–2025. Secara umum, grafik memperlihatkan adanya peningkatan signifikan hingga mencapai titik puncak pada tahun 2022, sebelum mengalami penurunan pada tahun-tahun berikutnya. Kenaikan tajam tersebut mencerminkan eskalasi ancaman *phishing* yang semakin kompleks dan berdampak besar terhadap industri keuangan, sementara *tren* penurunan setelah 2022 menunjukkan mulai berkurangnya nilai kerugian meskipun kasus *phishing* masih terus terjadi.

Dalam kurun waktu tujuh tahun terakhir, tepatnya 2018-2025, Singapura berulang kali menghadapi kasus *phishing* yang merugikan industri keuangan. Berdasarkan laporan berita STOMP, pada tahun 2019 hingga 2020, nasabah POSB Bank melalui email yang tampak resmi dari bank, memberitahukan bahwa token digital *mobile banking* mereka akan kedaluwarsa. Kemudian, korban diarahkan untuk mengklik tautan yang membawa mereka ke situs web palsu akibatnya informasi / data login mereka dicuri, dan lebih dari S$172.000 diambil dari rekening nasabah tersebut (STOMP, 2018). Kasus ini menunjukkan bagaimana *phishing* menggunakan ketidakwaspadaan konsumen untuk mengirim email atau pesan palsu yang terlihat seperti asli dan sah.

Kasus lainnya, pada tahun 2021 terjadi 477 kasus *phishing* yang melibatkan sistem pembayaran instan *PayNow* di Singapura. Dalam modus operandi ini, korban menerima pesan yang mengklaim bahwa mereka telah menerima transfer uang dan diarahkan ke situs web palsu untuk mengklaim dana tersebut. Rata-rata setiap korban kehilangan sekitar S$3.400. Fenomena ini menunjukkan bagaimana penipu semakin canggih dalam memanfaatkan *platform* pembayaran digital populer untuk menargetkan korban (The Straits Times, 2022).

Pada Juni hingga Juli 2025, Citibank Singapura melaporkan sembilan kasus *phishing* di mana pelaku menyamar sebagai staf bank, menghubungi korban melalui telepon atau pesan instan, dan meminta informasi pribadi atau melakukan transfer dana. Total kerugian mencapai

S$153.000 (Singapore Police Force, 2025b). Kasus ini memperlihatkan bahwa walaupun bank meningkatkan edukasi dan sistem keamanan, penipuan *phishing* terus berevolusi dengan metode yang lebih kompleks.

Kasus besar terjadi pada OCBC Bank Singapura yang terjadi pada Desember 2021, dengan puncak serangan berlangsung selama sekitar satu minggu, yaitu dari 23 Desember 2021 hingga 30 Desember 2021. Berdasarkan publikasi oleh *Singapore Police Force* 2023, dalam kasus ini pelaku mengirimkan SMS palsu yang mengaku dari bank, memperingatkan korban tentang upaya akses tidak sah, dan meminta mereka mengeklik tautan untuk verifikasi. Setelah mengklik, korban diarahkan ke situs palsu yang meminta kredensial perbankan serta OTP, yang kemudian digunakan penipu untuk mencuri dana. Mengutip laporan dari berita *Channel New Asia* (CNA) pada tahun 2021, awalnya 469 nasabah mengalami kerugian sebesar S$8,5 juta atau sekitar 103,78 miliar rupiah, namun jumlah korban terus bertambah hingga mencapai 790 orang dengan total kerugian S$13,7 juta atau sekitar 167,51 miliar rupiah.

Dari data *Numbeo Crime Index* 2025, Singapura tercatat sebagai negara paling aman di kawasan dengan *Crime Index* terendah, yaitu 22,6, serta *Safety Index* tertinggi, yaitu 77,4, yang mencerminkan ketatnya penegakan hukum dan efektivitas sistem keamanan nasional (Numbeo, 2025). Namun, meskipun memiliki tingkat kriminalitas umum yang rendah, Singapura tetap menghadapi tantangan serius dari sisi kejahatan siber, khususnya *phishing*. Hal ini terlihat dari laporan *Singapore Police*

Force (2024) yang mencatat ribuan kasus *phishing* dengan kerugian mencapai jutaan dolar Singapura, sehingga memperlihatkan bahwa keamanan fisik tidak serta-merta menjamin bebas dari ancaman digital.

Secara keseluruhan, data global dan nasional menunjukkan bahwa *phishing* merupakan bentuk kejahatan siber yang paling agresif dan merugikan, terutama ketika menargetkan sektor perbankan. Secara global, sektor keuangan secara konsisten menjadi target utama *phishing* karena menyimpan data pribadi dan aset bernilai tinggi, serta memiliki tingkat kepercayaan publik yang besar. Kondisi ini juga tercermin di Singapura, di mana sekitar 63% upaya *phishing* secara langsung mengatasnamakan institusi keuangan dan perbankan (Jacob et al., 2025). Fakta ini menegaskan bahwa *phishing* di sektor perbankan bukanlah insiden yang bersifat sporadis, melainkan pola kejahatan sistematis yang memanfaatkan reputasi bank untuk mengecoh nasabah dan mengakses sumber daya finansial secara ilegal.

Tingkat keparahan *phishing* di Singapura semakin terlihat dari besarnya kerugian dan konsistensi kasus yang terjadi sepanjang 2018–2025. Ironisnya, kondisi ini terjadi di tengah citra Singapura sebagai negara dengan tingkat kriminalitas konvensional yang rendah dan sistem keamanan nasional yang kuat (Numbeo, 2025). Hal ini menunjukkan bahwa keamanan fisik dan penegakan hukum yang ketat tidak secara otomatis mampu melindungi industri keuangan dari ancaman digital berbasis rekayasa sosial. Dengan demikian, *phishing* di industri keuangan dapat dipahami sebagai

ancaman serius terhadap stabilitas keuangan digital dan kepercayaan publik, yang menuntut pendekatan penanganan tidak hanya berbasis teknis, tetapi juga penguatan literasi dan kesadaran keamanan siber secara sistemik.

2.2.5. Regulasi Nasional dan Kebijakan Keamanan Siber di Singapura

Singapura telah memiliki regulasi nasional yang komprehensif dalam bidang keamanan siber *melalui Cybersecurity Act 2018* (No. 9 of 2018). *Cybersecurity Act* 2018 ini menjadi dasar hukum nasional dalam mencegah, mengelola, dan menanggulangi ancaman siber. Di dalam *part* 3, *section* 7 Undang-Undang ini berisi memberikan kewenangan kepada *Commissioner of Cybersecurity* untuk menetapkan suatu sistem komputer sebagai *Critical Information Infrastructure* (CII) apabila gangguannya berpotensi menimbulkan dampak serius terhadap layanan penting negara. Selanjutnya, Section 14 mewajibkan pemilik atau operator CII untuk segera melaporkan setiap insiden siber, dan *Section* 15 mengatur kewajiban audit keamanan. Hal ini menunjukkan bahwa regulasi Singapura bersifat proaktif dengan menekankan aspek pencegahan, pelaporan, dan kepatuhan hukum bagi setiap operator infrastruktur penting .

Selain itu, *Cybersecurity Act* 2018 juga menegaskan peran otoritas dalam mengendalikan situasi darurat melalui *Part* 5, *Section* 24, yang memberikan kewenangan kepada *Commissioner* untuk mengeluarkan arahan darurat ketika serangan siber mengancam stabilitas nasional. Bagian ini juga dilengkapi dengan ketentuan investigasi yang tercantum dalam

Sections 25–28, yang mengharuskan operator untuk bekerja sama dalam penyelidikan insiden (Government of Singapore, 2018).

Cybersecurity Act 2018 di Singapura awalnya disahkan untuk memberikan dasar hukum yang kuat dalam melindungi CII, namun seiring perkembangan teknologi regulasi lama dinilai belum cukup menjawab risiko baru. Karena itu, pada Mei 2024 disahkan *Cybersecurity* (Amendment) Bill No. 15/2024. Substansi utamanya adalah memperluas cakupan regulasi agar sesuai dengan perkembangan tekonologi, seperti peningkatan penggunaan *cloud computing* dan risiko *supply chain attack*. Ada empat kategori baru yang diatur di dalam amandemen ini, yaitu *Third-Party-Owned* CII (TPO CII), *Major Foundational Digital Infrastructure* (FDI) *providers*, *Entities of Special Cybersecurity Interest* (ESCIs), dan *Systems of Temporary Cybersecurity Concern* (STCCs).

Selain itu, cakupan CII diperluas hingga ke sistem yang berada di luar Singapura jika terkait layanan esensial, dengan kewajiban tambahan pelaporan insiden, audit, serta kepatuhan standar keamanan. Amandemen 2024 juga memperkuat kewenangan *Commissioner of Cybersecurity*, termasuk pengawasan lebih ketat terhadap penyedia layanan keamanan siber berlisensi serta penerapan sanksi perdata hingga 10% dari omzet tahunan atau SGD 500.000 bagi pelanggar.

Selain regulasi hukum, Singapura juga telah memperkuat kebijakan melalui *Singapore Cybersecurity Strategy* 2016 yang sekarang telah diperbarui menjadi *Cybersecurity Strategy* 2021. Di dalamnya memuat

strategi yang menekankan 3 pilar utama yaitu, memperkuat pertahanan digital, membangun ekosistem keamanan siber yang tangguh, serta memperluas kerja sama internasional (CSA, 2021). Implementasinya tampak dalam kampanye literasi digital, aplikasi pencegahan penipuan seperti *ScamShield*, dan latihan tahunan yang melibatkan sektor publik maupun swasta. Menurut CSA (2023), strategi ini bertujuan menjaga kepercayaan publik terhadap ekosistem digital serta memastikan Singapura tetap menjadi pusat ekonomi digital yang aman di kawasan. Dengan kombinasi regulasi hukum yang jelas dan kebijakan strategis yang adaptif, Singapura menegaskan posisinya sebagai salah satu negara dengan tata kelola keamanan siber paling komprehensif di Asia Tenggara.

2.3. Literasi Digital Masyarakat melalui *Cybersecurity Awareness Campaign*

2.3.1 Program *Cybersecurity Awareness Campaign*

Program *Cybersecurity Awareness Campaign* merupakan inisiatif tahunan yang digagas oleh *Cyber Security Agency of Singapore* (CSA) untuk meningkatkan kesadaran publik terhadap ancaman kejahatan siber yang terus berkembang. Program kampanye ini memiliki tujuan untuk memberikan pengetahuan kepada masyarakat di Singapura tentang bagaimana cara melindungi diri dari serangan siber, termasuk kejahatan *phishing, malware*, dan penipuan *daring* lainnya. Bentuk kegiatan dari program kampanye ini meliputi penyebaran materi mengenai edukasi melalui media sosial, iklan publik, seminar, dan kerja sama dengan

komunitas lokal maupun sekolah-sekolah. Tujuan utamanya adalah mengajarkan kebiasaan masyarakat bagaimana menggunakan teknologi digital dengan aman setiap hari sehingga mereka dapat menjadi lapisan pertama pertahanan dalam menghadapi ancaman kejahatan siber. Dengan cara ini, Singapura menunjukkan upayanya untuk menciptakan budaya keamanan siber yang kuat sejak tingkat individu (CSA, 2025).

Selain aspek edukasi, kampanye ini dirancang secara inovatif agar lebih mudah diterima oleh masyarakt umum. CSA setiap tahun meluncurkan tema khusus, seperti *"Better Cyber Safe than Sorry"* yang menunjukkan betapa pentingnya menjaga keamanan digital dalam kehidupan sehari-hari. Materi dari kampanye ini biasanya mengandung instruksi sederhana seperti cara memverifikasi tautan, mengidentifikasi pesan mencurigakan, dan menjaga kerahasiaan dari kata sandi milik individu. Menurut laporan dari CSA (2023), program kampanye ini telah menjangkau jutaan pengguna internet Singapura melalui berbagai kanal komunikasi. Singapura menegaskan bahwa peningkatan literasi digital adalah bagian terpenting dari strategi pencegahan *phishing* dan ancaman siber lainnya dengan keberlanjutan dari program kampanye ini.

2.3.2 Program *Cybersecurity Awareness Campaign* yaitu Kampanye *"Better Cyber Safe than Sorry"*

Program *Cybersecurity Awarness Camapaign* di Singapura diwujudkan melalui kampanye "*Better Cyber Safe than Sorry*" untuk meningkatkan kesadaran masyarakat, terutama pelajar, tentang pentingnya

menerapkan praktik keamanan siber yang baik dalam kehidupan sehari-hari. Kampanaye "*Better Cyber Safe than Sorry*" menggunakan pendekatan inovatif melalui media luar ruang, digital, dan media siaran gratis untuk bisa menjangkau audiens yang lebih luas. Kampanye ini menekankan empat praktik utama untuk keamanan siber : (1) menggunakan kata sandi yang kuat dan mengaktifkan autentikasi dua factor (2FA); (2) mengidentifikasi tanda-tanda *phishing*; (3) menggunakan perangkat lunak antivirus; (4) memperbarui perangkat lunak secara rutin. Setiap praktik diilustrasikan dengan analogi dari kehidupan sehari-hari agar mudah untuk dipahami oleh masyarakat. Salah satu contohnya adalah membandingkan penggunaan kata sandi yang kuat dengan mengunci pintu rumah untuk melindungi dari penyusup (CSA, 2018).

Selain itu, sebagai bagian dari kampanye "*Better Cyber Safe than Sorry*", CSA turut meluncurkan video musik berdurasi tiga menit yang menampilkan Jaga1, maskot keamanan siber yang dikembangkan oleh *Government Technology Agency* (GovTech). Tujuan dari video ini adalah untuk menarik perhatian pelajar dan mendorong mereka untuk menggunakan praktik keamanan siber yang baik. CSA juga menyelenggarakan *#BetterCyberSafeSG School Dance Challenge*, di mana siswa diminta untuk mengunggah video di mana mereka menari dan kemudian mengubah lagu dari video musik tersebut dengan cara yang kreatif. Tujuan dari kampanye ini adalah untuk mendorong pelajar untuk lebih aktif mempelajari dan menyebarkan tentang keamanan siber yang

sangat penting. Melalui kampanye yang dilaksanakan ini, CSA berharap dapat memberikan pengetahuan dan keterampilan yang diperlukan untuk menjaga keamanan pribadi mereka di internet kepada generasi muda serta mendorong mereka untuk berbagi informasi tersebut dengan teman dan keluarga.

Gambar 2. 2 Kampanye *"Better Cyber Safe than Sorry"* di Web Resmi CSA

Sumber: Cyber Security Agency of Singapore (CSA), 2021

Gambar tersebut merupakan salah satu dari berbagai materi edukatif yang mencakup perlindungan dan keamanan siber untuk meningkatkan literasi keamanan digital. Materi kampanye yang edukatif ini merupakan implementasi dari kampanye "*Better Cyber Safe than Sorry*" yang dapat diakses oleh masyarakat luas. Berdasarkan informasi dari *Cyber Security*

*Agency of Singapore (*CSA), sasaran dari program ini ditargetkan pada seluruh lapisan masyarakat, termasuk pelajar, aparatur, maupun pengguna internet pada umumnya. Oleh karena itu, implementasi dari kampanye ini disebarkan melalui berbagai platform resmi CSA agar pesan mengenai kewaspadaan terhadap ancaman *phishing* dapat tersampaikan secara efektif ke masyarakat.

Oleh karena itu, penting untuk menelaah lebih dalam bagaimana kapasitas institusional *Cyber Security Agency of Singapore* (CSA) dalam meningkatkan literasi keamanan digital masyarakat mampu membentuk pola kewaspadaan yang konsisten dan berkelanjutan terhadap serangan *phishing,*