Jurnal Komunikasi: Malaysian Journal of Communication
https://ejournal.ukm.my/mjc
Volume 42(1) 2026: 268-287

Pengurusan Keselamatan Siber Perbankan Internet di Malaysia melalui Pendekatan Teknologi dan Komunikasi Risiko

MUHAMMAD ADNAN PITCHAN*
NUR IZZAH 'ATIRAH ABDUL RAHIM
Universiti Kebangsaan Malaysia

SITI NUR HUSNA ABD RAHMAN
Universiti Teknologi MARA (UiTM), Malaysia

ABSTRAK

Transformasi perbankan digital telah menjadikan institusi perbankan sebagai aktor penting dalam pengurusan risiko keselamatan siber. Namun, peningkatan insiden jenayah siber seperti kehilangan wang tanpa disedari, serangan *phishing* dan kecurian identiti menunjukkan wujudnya jurang antara kecanggihan teknologi keselamatan perbankan dengan keberkesanan pengurusan risiko serta komunikasi keselamatan kepada pengguna. Walaupun institusi perbankan menekankan pematuhan piawaian dan sistem keselamatan yang canggih, pendekatan berorientasikan teknologi semata-mata didapati masih tidak mencukupi untuk menangani ancaman siber yang semakin kompleks dan sekali gus menjejaskan kepercayaan pengguna terhadap perbankan internet. Sehubungan itu, artikel ini bertujuan mengenal pasti isu utama keselamatan siber dalam perbankan internet di Malaysia, menganalisis peranan institusi perbankan dalam menangani ancaman tersebut serta meneliti cabaran strategik yang membataskan keberkesanan perlindungan pengguna. Kajian ini menggunakan pendekatan kualitatif melalui temu bual mendalam bersama enam orang informan daripada institusi perbankan terpilih di Kuala Lumpur yang melibatkan RHB Bank Berhad, CIMB Bank Berhad dan Affin Bank Berhad. Data dianalisis secara tematik bagi mengenal pasti pola dan cabaran institusi dalam pengurusan keselamatan siber perbankan. Dapatan kajian menunjukkan bahawa keselamatan siber perbankan terbentuk melalui interaksi kompleks antara kelemahan sistem, kecuaian pengguna, jurang literasi digital serta keterbatasan komunikasi keselamatan. Selain itu, strategi komunikasi keselamatan yang bergantung kepada laman sesawang didapati kurang selari dengan corak penggunaan aplikasi perbankan mudah alih. Kajian ini mencadangkan agar pengurusan keselamatan siber perbankan beralih daripada pendekatan teknikal semata-mata kepada kerangka pengurusan risiko yang menekankan komunikasi strategik, pendidikan pengguna dan akauntabiliti institusi.

Kata kunci*: Keselamatan siber perbankan, komunikasi risiko, jenayah siber, literasi digital pengguna, kepercayaan institusi.*

Managing Internet Banking Cybersecurity in Malaysia through Technological Approaches and Risk Communication

ABSTRACT

The transformation of digital banking has positioned banking institutions as key actors in managing cyber risk communication. However, the increasing number of cybercrime incidents such as unauthorized fund transfers, phishing attacks and identity theft reveals a gap between the advancement of banking security technologies and the effectiveness of risk management and security

*Corresponding author: adnan86@ukm.edu.my
E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4201-15
Received: 10 February 2026 | Accepted: 16 March 2026 | Published: 31 March 2026

communication to users. Although banking institutions emphasise compliance with security standards and advanced technological systems, technology driven approaches alone remain insufficient to address increasingly complex cyber threats, which may undermine users' trust in internet banking services. This article aims to identify key cybersecurity issues in internet banking in Malaysia, analyse the role of banking institutions in addressing these threats, and examine strategic challenges that limit the effectiveness of user protection. This study adopts a qualitative approach through in-depth interviews with six informants from selected banking institutions in Kuala Lumpur, namely RHB Bank Berhad, CIMB Bank Berhad and Affin Bank Berhad. The data were analysed thematically to identify patterns and institutional challenges in managing banking cybersecurity. The findings show that cybersecurity issues arise from interactions between system vulnerabilities, user negligence, gaps in digital literacy and limitations in security communication. The study also finds that security communication strategies relying mainly on websites are inconsistent with users' reliance on mobile banking applications. The study suggests that cybersecurity management should move beyond purely technical approaches towards a framework emphasising strategic communication, user education and institutional accountability.

Keywords: *Banking cybersecurity, risk communication, cybercrime, user digital literacy, institutional trust.*

PENGENALAN

Perkembangan teknologi komunikasi telah menjadikan dunia siber sebagai medium utama yang mempengaruhi hampir keseluruhan aspek kehidupan manusia, khususnya dalam urusan kewangan dan transaksi harian. Penggunaan transaksi maya atau transaksi berasaskan internet telah meningkat secara signifikan dan membawa kepada perubahan besar dalam landskap perbankan moden, sekali gus menghasilkan cabaran keselamatan siber yang semakin kompleks (Jafri et al., 2023). Di Malaysia, kadar penembusan pengguna perbankan internet telah meningkat kepada 107.4% berbanding 92.8% pada Julai 2019 dan 88.2% pada Julai 2018 (Bank Negara Malaysia, 2020). Menurut laporan Bank Negara Malaysia (2021), kadar penembusan pasaran perbankan internet terus meningkat sehingga 115.2%, sekali gus mencerminkan tahap kebergantungan masyarakat yang tinggi terhadap sistem perbankan digital.

Namun demikian, kepesatan transformasi digital dalam sektor perbankan turut membuka ruang kepada peningkatan ancaman jenayah siber. Isu keselamatan siber bukan lagi fenomena baharu, sebaliknya merupakan isu global yang melibatkan semua negara tanpa mengira tahap pembangunan. Kajian literatur antarabangsa menunjukkan bahawa perbankan digital sentiasa menjadi sasaran utama serangan siber seperti *phishing*, malware dan serangan tidak sah yang membawa kepada kerugian kewangan dan menjejaskan kepercayaan pengguna (Waliullah et al., 2025). Statistik tempatan turut mengesahkan trend ini, dengan statistik Jabatan Siasatan Jenayah Komersial (JSJK) Polis Diraja Malaysia merekodkan sebanyak 19,224 kes jenayah siber bagi tempoh Januari hingga September 2023 dengan jumlah kerugian mencecah RM687 juta (Nie, 2023). Selain itu, Suruhanjaya Komunikasi dan Multimedia Malaysia melaporkan sebanyak 1,764 laman sesawang palsu berkaitan penipuan pancingan data telah disekat antara Januari hingga Oktober 2023.

Kekerapan insiden keselamatan siber yang semakin meningkat termasuk kes kehilangan wang daripada akaun bank tanpa disedari telah menimbulkan kebimbangan serius dalam kalangan masyarakat dan secara langsung menjejaskan tahap kepercayaan pengguna terhadap sistem perbankan internet. Sebagai contoh, kes tular melibatkan seorang doktor pakar perubatan yang kehilangan wang sebanyak RM13,000 daripada akaun CIMB telah

mencetuskan persoalan awam mengenai keberkesanan keselamatan perbankan internet di Malaysia. Dalam konteks ini, transformasi penyampaian digital dalam sektor perbankan telah mengubah corak interaksi pengguna daripada urusan bersemuka di kaunter bank kepada penggunaan platform perbankan internet dan aplikasi mudah alih.

Seiring dengan perkembangan ini, penerapan standard keselamatan yang tinggi menjadi keperluan kritikal kepada institusi perbankan. Walau bagaimanapun, tahap keyakinan dan kepercayaan pengguna terhadap perbankan internet masih dipengaruhi oleh kelemahan sistem, isu keselamatan data peribadi serta kegagalan pencegahan ancaman siber secara menyeluruh. Faktor kepercayaan ini juga dikenal pasti dalam kajian lain sebagai elemen penting yang mempengaruhi perilaku pengguna dan keutamaan keselamatan dalam perbankan digital (Hassan et al., 2025). Menurut CyberSecurity Malaysia (2025), antara jenayah siber tertinggi di Malaysia ialah yang melibatkan penipuan, pencerobohan, gangguan siber, perisian hasad dan insiden berkaitan kandungan. Selain itu, Manoharan et al. (2022) menyatakan bahawa institusi perbankan kerap mengeluarkan amaran berkaitan laman web palsu yang direka untuk mencuri maklumat perbankan pelanggan menunjukkan bahawa sistem perbankan internet kekal sebagai sasaran utama penjenayah siber.

Dalam konteks ini, isu keselamatan siber perbankan internet bukan sahaja berpunca daripada keterbatasan teknologi atau kelemahan sistem keselamatan, tetapi turut melibatkan kegagalan dalam komunikasi risiko iaitu proses penyampaian maklumat keselamatan kepada pengguna secara berkesan untuk mempengaruhi tahap kesedaran, tingkah laku dan keyakinan mereka terhadap perkhidmatan (Waliullah et al., 2025). Kegagalan ini memberi impak terhadap persepsi risiko pengguna, terutama apabila mesej keselamatan tidak disampaikan melalui saluran yang konsisten dengan gaya penggunaan harian mereka. Berdasarkan kerangka pengurusan risiko siber terkini, pendekatan yang berkesan perlu menggabungkan aspek teknologi, proses, dan komunikasi strategik untuk meningkatkan perlindungan serta keyakinan pengguna terhadap perbankan digital (Azura et al., 2025). Sehubungan itu, artikel ini bertujuan untuk menilai pengurusan ancaman siber oleh institusi perbankan serta cabaran strategik yang menjejaskan perlindungan pengguna dan sistem digital.

SOROTAN LITERATUR

Secara umumnya, jenayah merujuk kepada perbuatan yang menyalahi undang-undang sama ada dilakukan secara sengaja atau tidak sengaja oleh individu atau kumpulan bagi mendapatkan maklumat atau keuntungan secara tidak sah (Mohd Fuad & Mohd Yusof, 2022). Dalam konteks teknologi maklumat, istilah siber merujuk kepada dunia maya atau persekitaran internet yang membolehkan pelbagai bentuk interaksi dan transaksi digital berlaku tanpa sempadan geografi. Perkembangan teknologi internet yang pesat telah membuka ruang kepada pelbagai bentuk jenayah siber, termasuk jenayah komputer yang melibatkan manipulasi sistem atau penyalahgunaan maklumat digital. Sebagai contoh, kewujudan laman sesawang palsu yang menyerupai laman rasmi institusi perbankan boleh digunakan untuk memperdaya pengguna bagi mendapatkan maklumat log masuk atau mengakses akaun perbankan internet mereka secara tidak sah.

Perkembangan teknologi digital turut mendorong peningkatan penggunaan perbankan internet dan perbankan mudah alih dalam kalangan pengguna. Kajian Lim et al. (2025) menunjukkan satu paradoks penting dalam penggunaan perbankan digital, iaitu walaupun isu keselamatan sering dibangkitkan dalam wacana perbankan internet, pengguna masih menunjukkan kecenderungan tinggi untuk menggunakan perbankan mudah alih disebabkan

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4201-15

faktor kemudahan, kegunaan dan pengaruh sosial. Dapatan ini menunjukkan bahawa kebimbangan terhadap keselamatan tidak semestinya menjadi faktor utama yang menentukan penggunaan teknologi perbankan digital, sekali gus mendedahkan jurang antara tahap kesedaran keselamatan dengan tingkah laku sebenar pengguna dalam persekitaran perbankan digital.

Selari dengan dapatan tersebut, Arif dan Masdupi (2020) menegaskan bahawa perbankan internet telah menjadi satu keperluan strategik bagi institusi perbankan untuk mengekalkan hubungan dengan pelanggan melalui penyediaan perkhidmatan yang pantas, mudah dan efisien. Walau bagaimanapun, penekanan terhadap kemudahan dan kecekapan perkhidmatan ini secara tidak langsung meningkatkan kebergantungan pengguna terhadap teknologi internet, sekali gus memperluas ruang pendedahan kepada ancaman keselamatan siber.

Dari perspektif keselamatan dan privasi, kajian Muhammad (2021) menekankan bahawa aspek ini merupakan elemen kritikal dalam operasi perbankan, khususnya dalam memastikan keyakinan pengguna terhadap sistem perbankan digital. Walaupun institusi perbankan bertanggungjawab menyediakan sistem keselamatan yang kukuh serta melaksanakan langkah perlindungan yang proaktif, keberkesanan pengurusan keselamatan perbankan internet tidak boleh bergantung kepada institusi semata-mata. Sebaliknya, ia memerlukan penglibatan aktif pengguna melalui tahap kesedaran, kefahaman serta amalan keselamatan yang berterusan dalam mengendalikan transaksi digital.

Dalam masa yang sama, perkembangan pesat teknologi kewangan digital turut meningkatkan kompleksiti ancaman keselamatan siber dalam sektor perbankan. Kajian literatur sistematik oleh Waliullah et al. (2025) mendapati bahawa peningkatan penggunaan perbankan digital telah mendedahkan pengguna dan institusi kewangan kepada pelbagai ancaman siber seperti *phishing, malware*, pencerobohan data serta akses tanpa kebenaran. Walaupun pelbagai teknologi keselamatan seperti pengesahan pelbagai faktor dan sistem pengesanan penipuan telah diperkenalkan, ancaman siber terus berkembang seiring dengan kemajuan teknologi digital.

Selain itu, aspek kesedaran keselamatan siber dan literasi digital turut memainkan peranan penting dalam mempengaruhi penggunaan perbankan digital. Kajian oleh Al-Doghan dan Mirzaliev (2024) menunjukkan bahawa kesedaran keselamatan siber, inovasi peribadi dan kemudahan akses mempunyai pengaruh signifikan terhadap tahap kepercayaan pengguna terhadap sistem perbankan digital. Kajian tersebut juga mendapati bahawa literasi digital berfungsi sebagai faktor moderator yang mengukuhkan hubungan antara kesedaran keselamatan dan penerimaan perbankan digital. Dalam konteks yang sama, Wei et al. (2025) menunjukkan bahawa niat penggunaan perkhidmatan *fintech* dipengaruhi oleh interaksi antara persepsi nilai dan persepsi risiko pengguna. Walaupun kemudahan teknologi menjadi faktor pendorong utama penggunaan perbankan digital, kebimbangan terhadap risiko keselamatan masih kekal sebagai faktor penting yang mempengaruhi penerimaan pengguna terhadap teknologi kewangan.

Secara keseluruhannya, sorotan literatur menunjukkan bahawa keselamatan perbankan internet bukan sahaja berkait dengan aspek teknologi tetapi turut melibatkan dimensi tingkah laku pengguna, kesedaran keselamatan serta tahap kepercayaan terhadap institusi perbankan. Walaupun banyak kajian terdahulu meneliti isu keselamatan siber dari perspektif teknologi dan penerimaan pengguna terhadap perbankan digital, kajian yang meneliti peranan institusi perbankan dalam mengurus keselamatan siber melalui pendekatan

komunikasi risiko masih terhad, khususnya dalam konteks Malaysia. Oleh itu, terdapat keperluan untuk meneroka dengan lebih mendalam bagaimana institusi perbankan mengurus isu keselamatan siber bukan sahaja dari sudut teknologi, tetapi juga melalui strategi komunikasi keselamatan yang berkesan dalam meningkatkan kesedaran serta perlindungan pengguna perbankan internet.

KAEDAH KAJIAN

Kaedah penyelidikan kualitatif digunakan untuk mengumpul data dalam kajian ini. Pendekatan ini mempunyai bentuk data yang tersendiri dari segi jawapan yang diperolehi daripada informan. Di bawah pendekatan kualitatif, kaedah temu bual mendalam telah dipilih untuk mendapatkan data kajian. Semua informan dalam kajian ini telah ditemu bual secara dalam talian yang mana proses ini mengambil masa selama 45 minit ke 1 jam. Semua perbualan bersama informan telah direkodkan dalam *Google Meet* dengan kebenaran para informan dan catatan tambahan juga telah direkodkan dalam buku nota semasa temu bual.

Lokasi dan Persampelan Kajian

Sebanyak 3 buah bank dari lokasi Kuala Lumpur telah dipilih dalam kajian ini iaitu RHB Bank Berhad, CIMB Bank Berhad dan Affin Bank Berhad. Antara kriteria yang telah diambil kira dalam pemilihan tiga buah bank ini ialah tahap keselamatan; insiden kehilangan kewangan pelanggan serta tanggungjawab bank terhadap masyarakat. Jumlah informan yang terlibat dalam kajian ini adalah seramai 6 orang informan yang dipilih secara bertujuan. Jumlah ini telah berhenti apabila data kajian telah mencapai tahap ketepuan. Jadual 1 menunjukkan maklumat informan kajian;

Jadual 1: Maklumat persampelan informan temu bual mendalam

Jumlah Informan	Bank	Lokasi
1	RHB Bank Berhad	Kuala Lumpur
2	RHB Bank Berhad	Kuala Lumpur
3	CIMB Bank Berhad	Kuala Lumpur
4	CIMB Bank Berhad	Kuala Lumpur
5	Affin Bank Berhad	Kuala Lumpur
6	Affin Bank Berhad	Kuala Lumpur

Pengumpulan dan Penganalisisan Data Temu Bual Mendalam

Langkah pertama di dalam proses ini adalah pencarian informan iaitu 6 orang informan daripada tiga institusi perbankan. Selepas pemilihan informan, proses seterusnya adalah pelantikan moderator yang mana dalam kajian ini pengkaji sendiri menjadi moderator dan mengendalikan proses perbincangan temu bual mendalam. Sesi suai kenal juga turut diadakan agar informan dan moderator saling mengenali satu sama lain. Sebelum sesi temu bual bermula, para informan telah diberikan taklimat ringkas tentang tujuan kajian ini dijalankan serta setiap informan diberi satu risalah maklumat kajian yang memperihal tentang tujuan, prosedur dan etika kajian. Apabila informan telah faham dan bersetuju, informan juga telah menandatangani borang persetujuan atau keizinan peserta kajian. Di akhir perbincangan, pengkaji memberikan tanda penghargaan kepada informan kerana sudi memberi kerjasama dan mengambil bahagian dalam kajian ini. Data yang dirakam telah ditranskripkan untuk proses penganalisisan iaitu satu langkah penting dalam mencari tema dan makna berdasarkan objektif kajian.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4201-15

HASIL DAPATAN DAN PERBINCANGAN KAJIAN

Profil Informan Kumpulan Fokus

Jadual 2 menunjukkan tentang demografi informan temu bual mendalam. Jumlah informan adalah seramai 6 orang yang mana 2 orang daripada RHB Bank Berhad, 2 orang informan daripada CIMB Bank Berhad dan dua lagi daripada Affin Bank Berhad. Majoriti informan adalah dalam kalangan perempuan iaitu 83.3 peratus dan lelaki 16.3 peratus. Informan paling tertua ialah berumur 47 tahun dan paling muda ialah 27 tahun. Kebanyakan informan juga mempunyai pengalaman kerja melebihi 5 tahun dan hanya seorang sahaja mempunyai pengalaman kerja 4 tahun iaitu informan 4.

Jadual 2: Demografi informan temu bual mendalam

Bil. Informan	Umur	Jantina	Bank	Tahap Pendidikan	Tempoh Perkhidmatan
1.	32 tahun	Lelaki	RHB Bank Berhad	Ijazah Sarjana Muda	8 Tahun
2.	47 tahun	Perempuan	RHB Bank Berhad	Diploma	11 Tahun
3.	32 tahun	Perempuan	CIMB Bank Berhad	Ijazah Sarjana Muda	6 Tahun
4.	27 tahun	Perempuan	CIMB Bank Berhad	Ijazah Sarjana Muda	4 Tahun
5.	46 tahun	Perempuan	Affin Bank Berhad	Diploma	20 Tahun
6.	36 tahun	Perempuan	Affin Bank Berhad	Ijazah Sarjana Muda	14 Tahun

Isu Utama Keselamatan Perbankan Internet di Malaysia

Berdasarkan analisis temubual bersama para informan dalam sektor perbankan dapatan kajian ini merumuskan beberapa isu utama berkaitan keselamatan siber dalam perbankan internet di Malaysia.

a) Kehilangan Wang Tanpa Disedari

Salah satu isu paling utama dalam perbankan internet di Malaysia adalah kehilangan wang secara misteri daripada akaun pengguna tanpa disedari oleh pemilik akaun. Dapatan kajian menunjukkan bahawa para informan menyatakan isu ini sebagai aduan yang paling kerap diterima daripada pelanggan mereka. Sebagai contoh informan TM1 menyatakan bahawa "Isu yang sering terjadi dan kami terima aduan pasal kehilangan duit di dalam akaun bank tanpa disedari," manakala informan TM2 pula menegaskan bahawa "duit hilang dalam akaun tu paling tinggi masalah yang dihadapi oleh pemegang akaun." Dua kenyataan ini memberikan gambaran yang jelas bahawa masalah kehilangan wang bukan sahaja berlaku secara berulang, bahkan sudah menjadi kebimbangan utama dalam keselamatan perbankan digital.

Fenomena kehilangan wang secara tiba-tiba ini dipercayai berpunca daripada pelbagai bentuk serangan siber, termasuk penggodaman sistem, kecurian identiti pengguna dan kelemahan kawalan keselamatan dalam aplikasi perbankan itu sendiri. Walaupun tidak dinyatakan secara spesifik oleh para informan bagaimana transaksi tersebut berlaku, kenyataan mereka mencerminkan betapa mudahnya akaun pelanggan diceroboh sama ada melalui kelemahan teknikal atau akibat kecuaian pengguna itu sendiri.

Selain itu, isu ini juga menimbulkan persoalan penting terhadap kecekapan sistem keselamatan siber bank-bank di Malaysia dalam menangani risiko kehilangan wang pelanggan. Meskipun institusi kewangan sentiasa menambah baik ciri-ciri keselamatan mereka, insiden seperti ini menunjukkan bahawa tahap perlindungan yang ada masih belum mencukupi untuk menghadapi ancaman yang semakin kompleks. Jika isu ini tidak ditangani secara sistematik dan menyeluruh, ia boleh menghakis keyakinan masyarakat terhadap penggunaan sistem

perbankan digital dan sekali gus menjejaskan aspirasi negara ke arah ekonomi digital yang mapan. Perbincangan ini boleh dilihat melalui Rajah 1.

Naratif #TM1

"Isu yang sering terjadi dan kami terima aduan pasal kehilangan duit di dalam akaun bank tanpa disedari"

Naratif #TM2

"Duit hilang dalam akaun tu paling tinggi masalah yang dihadapi oleh pemegang akaun"

Rajah 1: Contoh naratif informan

b) Serangan Phishing

Serangan *phishing* atau pancingan data merupakan satu lagi isu keselamatan yang sangat membimbangkan dalam perbankan internet di Malaysia. Isu ini timbul apabila penjenayah siber meniru laman web rasmi bank dan memperdayakan pengguna untuk memberikan maklumat peribadi dan data perbankan mereka. Hal ini boleh dilihat melalui kenyataan informan kajian di Rajah 2.

Naratif #TM2

"Masalah *phishing* di mana laman web bank dipalsukan untuk mengaburi mata pengguna bagi mendapatkan maklumat akaun pelanggan kami"

Naratif #TM5

"*Phishing* ni memang susah nak kawal sebab dia orang tiru bulat-bulat laman web kami, pengguna pun keliru"

Rajah 2: Contoh naratif informan

Masyarakat tidak boleh memandang remeh terhadap isu *phishing* ini kerana ia melibatkan elemen penipuan psikologi yang mengeksploitasi kepercayaan pengguna terhadap jenama bank. Pautan palsu yang dihantar melalui SMS, e-mel, atau media sosial selalunya kelihatan sahih dan menjadikan pengguna cenderung untuk terpedaya. Namun begitu, kejayaan *phishing* juga sering dipengaruhi oleh kelemahan pengguna dari segi pengetahuan dan sikap berjaga-jaga. Dalam hal ini, pengguna seharusnya lebih berwaspada dan tidak sewenang-wenangnya memberikan maklumat akaun kepada mana-mana laman atau pihak yang mencurigakan walaupun lamanya kelihatan rasmi.

Secara umumnya, bank mempunyai kewajipan untuk menyebarkan maklumat keselamatan dengan lebih efektif serta memastikan laman dan sistem mereka tidak mudah ditiru oleh pihak ketiga. Misalnya, bank boleh memperkenalkan ciri keselamatan tambahan yang dapat mengesahkan kesahihan laman atau transaksi seperti penggunaan pelayar keselamatan terbina atau ikon keselamatan khas pada setiap komunikasi rasmi bank. Sementara itu, pengguna juga perlu lebih cakna terhadap teknik penipuan semasa dan tidak bergantung sepenuhnya kepada sistem keselamatan bank untuk melindungi diri mereka.

Tidak boleh menafikan, keberkesanan pencegahan *phishing* memerlukan kolaborasi erat antara industri perbankan, agensi penguatkuasaan siber dan pengguna itu sendiri. Kesedaran awam perlu digerakkan secara konsisten melalui kempen pendidikan digital terutamanya dalam kalangan kumpulan rentan seperti warga emas dan pengguna kurang celik

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4201-15

teknologi. Bank juga tidak boleh bergantung kepada saluran maklumat sedia ada semata-mata, tetapi perlu meneroka pendekatan baharu yang lebih mesra pengguna untuk memberi amaran dan bimbingan kepada pelanggan. Secara keseluruhannya, serangan *phishing* adalah ancaman dinamik yang tidak akan selesai hanya dengan penyelesaian teknikal tetapi memerlukan pendekatan holistik berasaskan tanggungjawab bersama.

c) Kecuaian Pengguna Sendiri

Isu seterusnya yang dihadapi oleh pihak bank di Malaysia ialah kecuaian pengguna dalam mengurus maklumat peribadi dan akses kepada akaun bank. Berdasarkan dapatan kajian, terdapat informan yang menekankan bahawa ramai pengguna menggunakan kata laluan yang lemah, tidak unik atau sama bagi beberapa akaun perbankan. Terdapat juga kes yang mana pengguna secara sengaja mendedahkan maklumat peribadi kepada pihak ketiga sama ada dalam bentuk perkongsian sukarela seperti keldai akaun atau tertipu dengan mesej palsu. Kesemua ini menjadikan pengguna sasaran mudah kepada penjenayah siber. Hal ini boleh dilihat melalui kenyataan para informan di Rajah 3.

Naratif #TM4

"Berkenaan dengan masalah keselamatan siber seperti duit hilang dalam akaun peribadi mereka ini kadang-kadang berpunca daripada penetapan kata laluan yang lemah dan mudah diakses… untuk mudahkan mereka, mereka letak *password* yang sama dengan bank-bank lain."

Naratif #TM6

"Ada setengah pengguna yang jadi keldai akaun dan berkongsi maklumat peribadi dekat orang lain"

Rajah 3: Contoh naratif informan

Walaupun institusi kewangan menyediakan pelbagai lapisan keselamatan, realitinya pengguna masih menjadi titik paling lemah dalam rantaian keselamatan siber. Dalam beberapa kes, pelanggan menjadi mangsa bukan kerana sistem bank yang tidak selamat tetapi kerana kelalaian mereka sendiri dalam memastikan maklumat peribadi kekal sulit. Tindakan menggunakan semula kata laluan, menyimpan maklumat akses dalam telefon pintar tanpa menggunakan kata kunci keselematan atau membuka pautan tanpa pengesahan boleh mendedahkan akaun mereka kepada risiko yang tinggi. Dalam konteks ini dapatan ini kelemahan bukan terletak pada teknologi tetapi pada faktor manusia.

Tidak boleh menafikan bukan semua pengguna mempunyai latar belakang teknologi atau pendedahan terhadap risiko keselamatan digital. Terdapat dalam kalangan mereka, khususnya golongan warga emas atau pelanggan yang kurang celik digital, tidak benar-benar memahami kepentingan keselamatan dalam talian. Dalam hal ini, tanggungjawab tidak boleh diletakkan sepenuhnya ke atas pengguna. Pihak bank wajar menyediakan sistem yang bukan sahaja selamat, tetapi juga mesra pengguna dan mampu membimbing pelanggan agar tidak melakukan kesilapan yang sama berulang kali. Ini termasuk memberikan amaran yang jelas, penggunaan antara muka aplikasi yang intuitif serta komunikasi berkala dalam bentuk yang mudah difahami.

Dari perspektif yang lebih luas, isu ini menggambarkan pentingnya pendekatan pendidikan keselamatan digital sebagai sebahagian daripada strategi keselamatan perbankan. Bank perlu memainkan peranan aktif bukan sahaja sebagai penyedia sistem keselamatan

tetapi juga sebagai penyampai maklumat yang mampu membentuk sikap berjaga-jaga dalam kalangan pengguna. Dalam jangka panjang, keselamatan siber tidak boleh ditanggung sebelah pihak semata-mata. Ia adalah tanggungjawab kolektif yang memerlukan penyelarasan antara teknologi, dasar keselamatan institusi, dan kesedaran pengguna itu sendiri.

d) Keterbatasan Sistem

Isu keselamatan perbankan internet bukan sahaja berkait rapat dengan kecuaian pengguna, tetapi juga berkisar kepada hakikat bahawa sistem teknologi yang digunakan oleh institusi perbankan tidak bersifat sempurna. Walaupun kebanyakan bank menyatakan bahawa mereka mempunyai sistem keselamatan yang canggih seperti *SecureTAC, Lock Clicks ID* dan sebagainya tetapi hasil kajian menunjukkan bahawa sistem tersebut masih mempunyai kelemahan tersendiri yang boleh dieksploitasi oleh penjenayah siber. Dalam temu bual, beberapa informan mengakui wujudnya ruang atau '*loophole*' dalam sistem yang dibangunkan oleh bank dan boleh membuka jalan kepada pencerobohan yang tidak dapat diramal. Hal ini boleh dilihat melalui kenyataan informan dalam Rajah 4.

Naratif #TM3

"Setiap inovasi pasti ada '*loophole*' ataupun cacat cela yang membolehkan sistem itu dieksploitasi"

Naratif #TM6

"Sehebat mana pun sistem perbankan itu, tetap kan ada cara yang dapat tembus sistem dan timbul isu perbankan internet itu"

Rajah 4: Contoh naratif informan

Memang tidak boleh menafikan bahawa institusi perbankan telah melabur dalam membangunkan sistem keselamatan digital masing-masing dan sebahagian besar ciri-ciri ini dilihat responsif kepada cabaran siber semasa. Walaupun begitu, dalam dunia digital yang sentiasa berubah dan berkembang, setiap inovasi yang baru selalunya turut membuka peluang kepada ancaman yang baru. Ia seperti perlumbaan tanpa noktah antara pembina sistem dengan penceroboh. Hal ini umpama, ketika satu kelemahan berjaya ditutup, muncul pula kaedah serangan yang lebih canggih dan situasi ini boleh dikatakan bahawa tiada sistem yang benar-benar kebal dalam menghadapi ancaman siber.

Dalam konteks ini, penambahbaikan sistem keselamatan perlu digerakkan secara berterusan dan bukan secara reaktif semata-mata. Dalam isu ini, bank bukan hanya perlu menambah ciri-ciri baru, tetapi perlu melibatkan pendekatan holistik yang merangkumi ujian kerentanan berkala, latihan pengurusan krisis siber serta kerjasama dengan agensi keselamatan siber negara. Pada masa yang sama, bank seharusnya mempunyai sikap ketelusan dan perlu mengakui sekiranya sistem mereka mempunyai sebarang kelemahan. Tindakan bank ini boleh membina kepercayaan dalam kalangan pelanggan mereka.

e) Isu Global dan Berkembang Seiring Kemajuan Teknologi

Dapatan lain yang diperolehi tentang isu perbankan ialah perkembangan global. Dalam landskap perbankan digital masa kini, isu keselamatan siber tidak lagi dilihat sebagai masalah bersifat domestik atau berskala kecil. Sebaliknya, ia merupakan cabaran global yang turut dihadapi oleh semua negara tanpa mengira negara maju mahupun membangun. Dapatan

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4201-15

kajian ini memperlihatkan bahawa para informan mengakui ancaman terhadap keselamatan perbankan internet bersifat merentas sempadan dan semakin kompleks dari semasa ke semasa. Dengan kata lain, masalah ini bukan hanya wujud kerana kelemahan sistem tempatan semata-mata tetapi turut didorong oleh evolusi serangan siber yang berlaku di seluruh dunia.

Selain itu, isu ini perlu dilihat dalam konteks ekosistem teknologi global yang terbuka dan saling bergantung. Hal ini kerana kemajuan sistem teknologi di satu lokasi turut mendorong penjenayah siber di lokasi lain untuk berevolusi dengan cepat. Malah, tidak jarang serangan terhadap sistem tempatan berpunca daripada aktor luar negara khususnya sindiket jenayah siber antarabangsa yang memiliki sumber kewangan, kepakaran teknikal serta rangkaian operasi yang tersusun. Justeru, meskipun pelbagai langkah keselamatan telah dibangunkan, informan mengakui bahawa sistem masih terdedah kepada pencerobohan. Hal ini bukan disebabkan kelemahan mutlak pada sistem sebaliknya kerana ancaman yang dihadapi kini melibatkan penggunaan teknologi dan strategi yang sangat canggih. Hal ini boleh dilihat melalui kenyataan para informan di Rajah 5.

Naratif #TM1

"Teknologi yang pesat…mereka lagi hebat dan ada pelbagai cara yang dapat menceroboh maklumat privasi mangsa"

Naratif #TM5

"Masalah ni bukan dekat Malaysia je… seluruh dunia tengah cari solusi untuk jenayah siber ni"

Rajah 5: Contoh naratif informan

Masyarakat perlu menyedari bahawa dunia siber hari ini tidak lagi terikat kepada sempadan geografi. Dalam realiti sebegini, isu keselamatan siber tidak boleh lagi dianggap sebagai tanggungjawab individu atau sesebuah institusi semata-mata. Institusi kewangan di Malaysia, khususnya bank-bank, tidak seharusnya bergantung sepenuhnya kepada sistem dalaman mereka dan sebaliknya mereka perlu membina jaringan kerjasama strategik dengan agensi keselamatan antarabangsa, penyedia teknologi global dan rakan institusi kewangan di rantau ini. Pada masa yang sama, pihak kerajaan dan pembuat dasar juga perlu memainkan peranan yang lebih aktif dalam mewujudkan kerangka dasar dan undang-undang yang sejajar dengan piawaian keselamatan global. Tanpa pendekatan yang menyeluruh dan rentas sempadan, ancaman siber akan terus menjadi masalah yang sukar ditangani secara bersendirian.

f) Kurangnya Kesedaran Keselamatan Pengguna

Isu lain yang diutarakan oleh para informan ialah berkaitan tentang kesedaran dalam kalangan pengguna sistem perbankan. Walaupun sistem keselamatan perbankan internet semakin canggih dari semasa ke semasa tetapi masih wujud satu jurang besar yang sering kali menjadi titik lemah kepada keseluruhan ekosistem iaitu tahap kesedaran pengguna yang rendah terhadap isu keselamatan siber. Berdasarkan dapatan kajian, para informan jelas menyatakan bahawa sebahagian besar pengguna tidak menunjukkan sikap berjaga-jaga ketika menggunakan platform perbankan dalam talian. Mereka lebih cenderung untuk mengambil mudah dari segi aspek keselamatan seperti mengongsikan maklumat peribadi, tidak

memeriksa semula sumber maklumat yang diterima dan hanya menekan pautan tanpa berfikir panjang. Hal ini dibuktikan melalui kenyataan para informan di Rajah 6.

Naratif #TM1

"Tapi kalau pengguna sendiri kurang berhati-hati boleh jadi punca benda-benda ni macam jenayah siber ni berlaku"

Naratif #TM3

"Kami dah buat macam-macam sistem sekuriti, tapi kalau pelanggan tak peka… tetap senang kena tipu"

Rajah 6: Contoh naratif informan

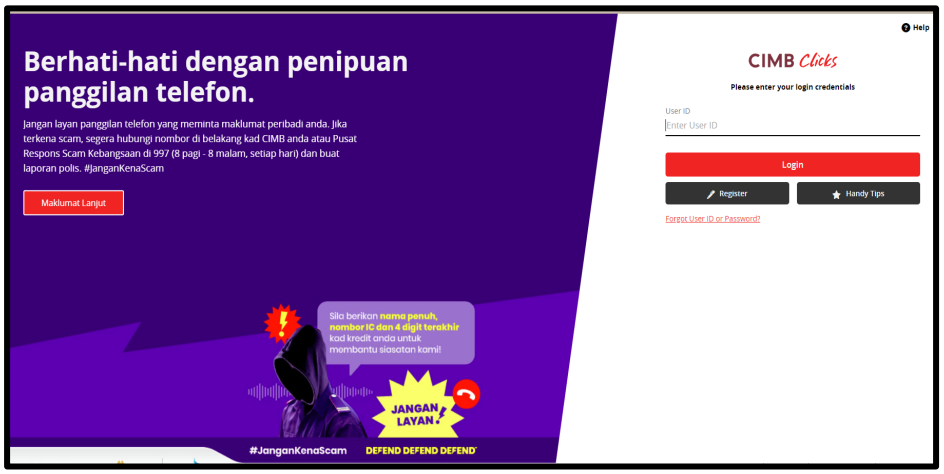
Hal ini lebih membimbangkan apabila terdapat dalam kalangan pengguna yang menganggap bahawa tanggungjawab keselamatan sepenuhnya terletak di bahu pihak bank. Mereka percaya bahawa sistem bank yang kukuh sudah mencukupi untuk melindungi diri mereka daripada sebarang bentuk serangan. Sikap pasif pengguna ini boleh membuka ruang kepada jenayah seperti pancingan data, kecurian identiti dan kehilangan wang. Dalam sesetengah kes, kelemahan ini bukan sepenuhnya berpunca daripada pengetahuan yang kurang tetapi disebabkan oleh sikap pengguna yang mengambil mudah terhadap risiko digital.

Peranan Pihak Bank Dalam Menangani Isu Keselamatan Siber

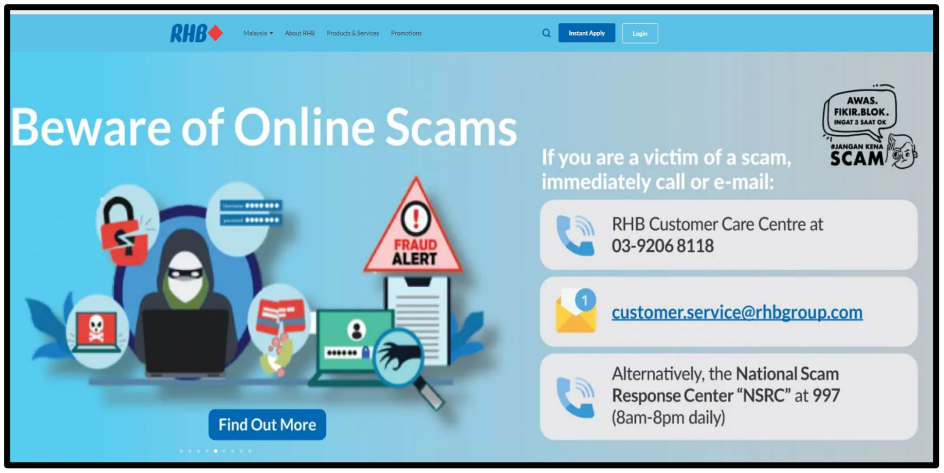
Bank memainkan peranan yang penting dalam mengatasi isu keselamatan siber terhadap perbankan internet. Dalam mempertingkatkan kesedaran pengguna perbankan internet terhadap keselematan siber peranan sektor perbankan adalah menjadi peranan utama untuk mengatasi isu-isu keselamatan siber terhadap perbankan internet. Hal ini kerana bank adalah sasaran penjenayah siber kerana sektor ini menyimpan maklumat kewangan dan aset berharga selain menjadi medium transaksi kewangan. Menurut INTERPOL (2020) daripada Data Penilaian Ancaman Siber Interpol Asean 2020 menunjukkan bahawa serangan pancingan data semakin meningkat dan sektor kewangan merupakan antara sasaran utama dalam serangan siber di rantau ASEAN. Oleh disebabkan itu, peranan bank amat penting dalam membantu mencegah daripada menjadi sasaran jenayah tersebut. Peranan pihak bank bukan sahaja melihat kepada penyampaian mesej kesedaran namun ia juga melibatkan tindakan serta merta yang diambil bagi membantu pelanggan yang sedang menghadapi masalah keselamatan siber yang mana tindakan pihak bank merujuk kepada pertolongan yang diberikan semasa berlakunya masalah yang melibatkan perbankan internet.

Bagi mengetahui peranan bank dalam isu keselamatan siber ini, tiga konstruk telah diajukan kepada para informan iaitu (i) penyampaian kesedaran isu keselamatan siber; (ii) dan tindakan yang diambil dalam membantu pengguna yang menghadapi masalah. Umumnya, laman sesawang setiap bank dipaparkan maklumat berkaitan kesedaran jenayah siber. Sebagai contoh, ketika pelanggan membuka laman sesawang perbankan *Cimb Clicks*, RHB akan dipaparkan mengenai kesedaran keselamatan jenayah penipuan seperti dalam Rajah 7, 8 dan 9. Ini adalah antara usaha pihak bank dalam mendidik pengguna mengenai keselamatan siber.

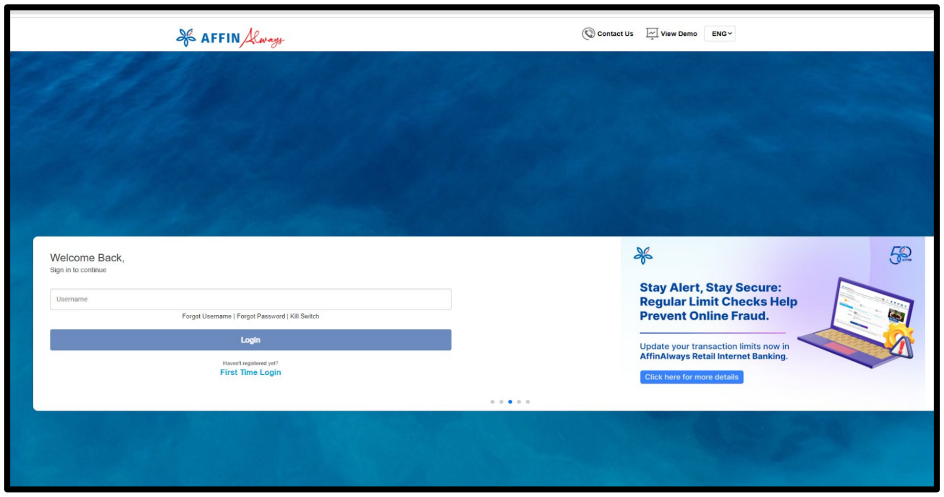
E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4201-15



Rajah 7: Paparan muka depan *Cimb Clicks*
Sumber: Laman sesawang CIMB



Rajah 8: Paparan muka depan *RHB Bank*
Sumber: Laman sesawang RHB



Rajah 9: Paparan muka depan *Affin Bank*
Sumber: Laman sesawang Affin

Namun begitu, dapatan kajian ini menunjukkan bahawa para informan menyatakan aspek kesedaran melalui laman sesawang masih belum mencukupi untuk mengelakkan isu keselamatan siber dalam perbankan internet. Berdasarkan Naratif TM4 dalam Rajah 10 turut menegaskan bahawa usaha bank dalam menyampaikan mesej keselamatan siber melalui laman web masih belum mencapai kesan yang diharapkan. Informan menyatakan bahawa walaupun laman sesawang bank telah menyediakan kandungan berbentuk kesedaran, namun "peranan yang kami lakukan tidak mencapai kepada pelanggan." Kenyataan ini menimbulkan persoalan tentang keberkesanan kaedah penyampaian mesej keselamatan yang sedia ada. Secara umumnya ia menunjukkan bahawa pendekatan yang bersifat satu hala dan terlalu bergantung kepada laman sesawang sebagai saluran utama tidak lagi sesuai dalam era digital yang memerlukan komunikasi lebih responsif, mudah dicapai dan mesra pengguna. Apabila bank sendiri menyedari bahawa mesej mereka tidak sampai, ini membuktikan bahawa wujud keperluan mendesak untuk menilai semula strategi komunikasi siber dengan memfokuskan kepada medium dan gaya penyampaian yang lebih dekat dengan amalan harian pelanggan.

Selain itu, Naratif TM5 yang dikemukakan dalam Rajah 10 menunjukkan bahawa pengguna perbankan internet bukan sahaja terdiri daripada golongan belia atau dewasa, malah turut melibatkan warga emas yang memerlukan panduan serta bantuan daripada individu yang lebih celik teknologi. Ini menggambarkan keperluan pendekatan komunikasi keselamatan siber yang lebih bersasar dan mesra pengguna, khususnya kepada golongan yang berisiko rendah dari aspek literasi digital. Hal ini turut mendedahkan kebarangkalian wujudnya jurang digital yang belum ditangani secara sistematik oleh kerajaan dan institusi perbankan, yang mana pelanggan tertentu menjadi bergantung kepada pihak ketiga untuk memahami kandungan keselamatan siber. Situasi ini meningkatkan kerentanan terhadap serangan siber sekiranya pihak ketiga tersebut juga tidak mengendahkan atau tidak memahami mesej yang disampaikan.

Naratif #TM4

"saya boleh katakan tidak cukup…memang laman web kami mungkin cukup nak bagi kesedaran membanteras jenaya siber…tapi masih peranan yang kami lakukan tidak mencapai kepada pelanggan".

Naratif #TM5

"contoh lah golongan tua yang tak pandai guna sistem perbankan internet…mesti dia kena mintak tolong anak dia ke … anak dia pun tak baca dan terus pangkah je...target kempen tidak tercapai".

Naratif #TM6

"*As for us, our customer* tak selalu pakai laman web, *because our bank* pelanggan banyak pakai aplikasi *Cimb Clicks* tu… jadi kebanyakan info pengguna perlu membuat carian sendiri untuk mendapatkan informasi berkaitan dengan *scammer* dan sebagainya ini"

Rajah 10: Contoh naratif informan

Naratif TM6 dalam Rajah 10 juga memperlihatkan bahawa kempen kesedaran yang diletakkan di papan muka laman sesawang bank kurang berkesan, terutamanya apabila pelanggan kini lebih cenderung menggunakan aplikasi perbankan mudah alih. Kecenderungan ini berpunca daripada kemudahan yang ditawarkan oleh aplikasi seperti *CIMB Clicks, i-Rakyat,*

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4201-15

RHB Mobile Banking yang membolehkan pengguna melakukan pelbagai transaksi dengan cepat dan mudah termasuk menyemak baki akaun, membuat pembayaran menggunakan kod QR, dan melihat sejarah transaksi. Oleh itu, aplikasi ini digunakan secara fokus untuk tujuan tertentu sahaja dan jarang sekali pengguna melayari laman sesawang bank kecuali jika perlu mendapatkan maklumat khusus atau menyelesaikan isu teknikal. Analisis dapatan ini menunjukkan bahawa bank kemungkinan belum menyelaraskan strategi komunikasi mereka dengan perubahan tingkah laku digital pengguna. Apabila maklumat keselamatan siber tidak disampaikan di tempat yang paling kerap diakses seperti dalam aplikasi bank, maka matlamat pendidikan keselamatan siber tidak akan tercapai. Ini mengakibatkan pengguna kekal berada dalam keadaan tidak sedar walaupun mereka berada dalam ekosistem digital bank yang sepatutnya melindungi mereka.

Hal ini menunjukkan bahawa peranan bank dalam mendidik pelanggan tentang keselamatan siber tidak boleh bergantung sepenuhnya kepada laman sesawang semata-mata. Maklumat penting berkaitan ancaman siber dan langkah pencegahannya perlu disampaikan secara lebih aktif dan terus kepada pengguna melalui medium yang mereka gunakan setiap hari seperti aplikasi perbankan mudah alih. Sekiranya maklumat hanya disediakan apabila pengguna 'mencari' atau melayari laman sesawang atas tujuan tertentu, maka mesej keselamatan tidak akan sampai kepada majoriti pengguna secara efektif. Hal ini membuktikan bahawa strategi komunikasi reaktif yang hanya menunggu pengguna datang mencari adalah tidak lagi sesuai dalam konteks perbankan digital semasa. Sebaliknya, bank perlu mengambil pendekatan proaktif dengan mengintegrasikan mesej keselamatan secara automatik dan berkala dalam aliran penggunaan aplikasi misalnya melalui *pop-up*, notifikasi atau video pendek dalam aplikasi. Hal ini bukan sahaja mampu meningkatkan kesedaran malah membantu membina sikap berhati-hati dalam kalangan pengguna selaras dengan peranan bank sebagai entiti yang bukan sahaja menyediakan perkhidmatan tetapi juga melindungi kesejahteraan digital pelanggan mereka.

Selain daripada itu, dalam situasi kecemasan melibatkan keselamatan siber tindakan pantas daripada pihak bank merupakan elemen penting dalam mengurangkan risiko kerugian yang lebih besar kepada pengguna. Dapatan kajian menunjukkan bahawa langkah pertama yang sering diambil oleh pengguna apabila menyedari sesuatu yang mencurigakan dalam akaun mereka ialah dengan menghubungi pusat panggilan bank. Saluran ini menjadi pilihan utama kerana ia menyediakan akses segera kepada bantuan dan bimbingan profesional dalam menangani isu yang timbul. Ia mencerminkan tahap kebergantungan pengguna terhadap kecekapan sistem sokongan pelanggan yang disediakan oleh pihak institusi kewangan.

Informan juga menyatakan sebaik sahaja pihak bank menerima aduan, bank akan mengambil tindakan yang pantas dengan membekukan akaun yang terlibat. Langkah ini diambil untuk menghalang sebarang transaksi lanjut yang boleh mengakibatkan kerugian tambahan. Tambahan pula, proses ini turut disertai dengan permintaan kepada pelanggan untuk menyediakan maklumat sokongan seperti butiran transaksi yang mencurigakan, mesej teks, e-mel atau sebarang bentuk komunikasi lain yang relevan. Kerjasama pelanggan dalam menyampaikan maklumat ini amat penting bagi memudahkan proses siasatan dalaman yang akan dijalankan oleh pihak bank. Ini juga menunjukkan bahawa proses mitigasi keselamatan tidak hanya terletak di bahu pihak bank tetapi turut memerlukan penglibatan aktif daripada pelanggan.

Selain pembekuan akaun, langkah susulan yang turut diambil oleh pihak bank ialah membatalkan kad kredit yang dimiliki oleh pelanggan serta membuat penyekatan akses kepada sistem perbankan dalam talian buat sementara waktu. Tindakan ini bertujuan untuk menutup sebarang ruang atau peluang yang mungkin digunakan oleh pihak tidak bertanggungjawab untuk meneruskan aktiviti jenayah siber. Pendekatan menyeluruh ini memperlihatkan bahawa pihak bank komited dalam melindungi keselamatan akaun pengguna dengan menyekat semua bentuk akses ke atas dana atau data pelanggan sehingga siasatan selesai dan tahap keselamatan dipulihkan sepenuhnya. Tambahan pula, kajian juga mendapati siasatan awal turut dijalankan oleh pihak bank sebagai sebahagian daripada prosedur pengesahan. Dalam proses ini, pelanggan akan diajukan beberapa soalan yang berfungsi sebagai bukti awal dan pengesahan terhadap dakwaan yang dibuat. Langkah ini penting untuk mendokumentasikan maklumat yang diperlukan sebelum kes tersebut dirujuk kepada pihak berkuasa.

Hal ini menunjukkan bahawa pihak bank telah mempunyai satu rangka kerja tindakan yang responsif dan sistematik dalam menghadapi isu keselamatan siber. Tindakan-tindakan tersebut memperlihatkan kecekapan operasi dan komitmen bank untuk melindungi pengguna bukan sahaja daripada kerugian kewangan tetapi juga daripada implikasi psikologi akibat serangan siber. Hal ini dibuktikan oleh kenyataan para informan dalam Rajah 11.

Naratif #TM1

"pusat panggilan akan menjadi sasaran utama… first mangsa akan buat mesti *call hotline* dulu .. maklumkan kepada pihak bank ada sebarang keraguan dalam akaun bank tu".

Naratif #TM3

"pihak khidmat pelanggan akan membekukan akaun bank terlebih dahulu.. *But the bank may also ask the customer to provide additional information, such as the details of the suspicious transaction, any relevant emails or text messages, and any other information that can help with the investigation*".

Naratif #TM4

"membatalkan segala kad kredit dan menyekat *online banking* buat sementara waktu".

Naratif #TM5

"sedikit soal siasat akan dibuat sebagai bukti".

Rajah 11: Contoh naratif informan

Cabaran Dihadapi Oleh Pihak Bank Dalam Mengatasi Isu Keselamatan Siber

Dalam era digital yang berkembang pesat, institusi perbankan bukan sahaja berdepan dengan keperluan untuk menyediakan perkhidmatan yang cekap dan mesra pengguna tetapi turut dihimpit oleh pelbagai cabaran keselamatan siber yang semakin kompleks. Hasil kajian mendapati terdapat beberapa cabaran yang telah diutarakan oleh informan;

a) Teknologi dan Kepakaran

Salah satu cabaran utama yang dihadapi oleh sektor perbankan dalam mengurus keselamatan siber ialah keperluan untuk mengikuti perkembangan teknologi yang sangat pesat. Bank perlu

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4201-15

sentiasa mengemas kini sistem keselamatan mereka agar dapat menyaingi taktik penjenayah siber yang semakin sofistikated. Dalam hal ini, bank bukan sahaja perlu melabur dalam peralatan dan infrastruktur teknologi maklumat yang canggih, tetapi juga memerlukan tenaga kerja yang mahir untuk mengendalikannya. Justeru, permintaan terhadap kepakaran ini mencetuskan cabaran tambahan kerana bidang keselamatan siber memerlukan kemahiran khusus dan sentiasa berubah selaras dengan landskap ancaman digital global.

Selain itu, institusi perbankan turut terikat dengan pelbagai peraturan dan garis panduan berkaitan keselamatan data dan privasi. Kewajipan untuk mematuhi keperluan perundangan ini telah meningkatkan tekanan terhadap institusi kewangan untuk menyediakan sistem keselamatan yang kukuh dan boleh dipercayai. Naratif TM3 dalam Rajah 12 juga memperlihatkan bahawa dalam usaha untuk memastikan pematuhan terhadap piawaian keselamatan, pihak bank terpaksa memperuntukkan sumber kewangan dan kepakaran yang besar, sekali gus membuktikan bahawa keperluan teknologi dan kepatuhan bukan sekadar perkara teknikal, malah merupakan beban pentadbiran dan strategik yang besar.

Cabaran ini juga membawa implikasi besar terhadap perancangan strategik bank. Kebergantungan terhadap kepakaran luar atau penyedia perkhidmatan keselamatan siber boleh menimbulkan isu kebergantungan teknologi asing, sementara keperluan melatih kakitangan dalaman memakan masa dan kos yang tinggi. Oleh itu, dalam usaha untuk mengekalkan tahap keselamatan yang tinggi, bank perlu bijak mengimbangi antara pelaburan dalam teknologi dan pembangunan sumber manusia, dengan memastikan strategi keselamatan mereka tetap lestari, fleksibel dan sesuai dengan cabaran semasa.

Naratif #TM3

"Kami perlu memenuhi keperluan patuh kepada peraturan dan garis panduan *related to security, data protection and privacy*. *So* untuk memenuhi keperluan ini menjadi cabaran dan memerlukan sumber kewangan dan kepakaran yang besar… untuk mencegah daripada masalah *cybercrime*".

Rajah 12: Contoh naratif informan

b) Internet Tanpa Sempadan dan Evolusi Penjenayah

Ciri asas internet yang tanpa sempadan, tanpa identiti tetap dan beroperasi dengan kelajuan tinggi menjadi cabaran yang sangat signifikan kepada institusi perbankan. Penjenayah siber hari ini tidak lagi beroperasi secara manual, tetapi menggunakan perisian automatik, penggodam sewaan dan teknik penipuan pintar yang sukar dikesan. Mereka terus menyesuaikan strategi dan kaedah serangan mereka mengikut perkembangan sistem bank, menjadikan tugas pihak bank untuk mengekang serangan siber sebagai usaha yang berterusan dan kompleks. Menurut naratif informan dalam Rajah 13 menunjukkan bahawa kewujudan internet tanpa batasan meletakkan institusi perbankan dalam keadaan sentiasa bersedia dan bertindak balas secara pantas bagi melindungi akaun dan data pelanggan mereka.

Cabaran ini bukan sahaja memerlukan bank melabur dalam sistem yang boleh mengesan dan menyekat serangan, tetapi juga memerlukan pemantauan secara berterusan ke atas semua aktiviti yang berlaku di dalam sistem. Oleh kerana ancaman sentiasa berkembang, sistem keselamatan juga perlu dikemas kini secara berkala, menyebabkan bank perlu mempunyai pasukan khas atau sistem automasi yang boleh mengenal pasti corak aktiviti yang luar biasa. Dalam konteks ini, pihak bank perlu bertindak lebih cekap daripada

penjenayah siber sendiri dan hal ini merupakan satu tuntutan yang amat mencabar kerana serangan boleh berlaku dari mana-mana negara dalam masa yang sangat singkat.

Selain itu, bank juga turut berdepan dengan cabaran untuk mengimbangi antara keselamatan dan kemudahan pengguna. Sistem yang terlalu ketat dan berlapis boleh menyukarkan pelanggan menjalankan transaksi harian, sekali gus mencetuskan rungutan dan ketidakselesaan. Namun, jika sistem terlalu longgar pula, risiko pencerobohan akan meningkat. Maka, bank berada dalam dilema untuk mengekalkan keselamatan tanpa menjejaskan pengalaman pengguna yang memerlukan pendekatan yang strategik, pragmatik dan berdasarkan analisis tingkah laku pengguna sebenar.

Naratif #TM1

"*Cybercriminals continue to develop new techniques for accessing financial information*… jadi cabaran kami sebab kewujudan internet tanpa batasan ni … kami perlu buat kerja yang lebih *which continuously monitors and updates the security systems to stay ahead of the criminals*".

Naratif #TM2

"*More security features because scammers are more efficient than banks. But not just that, the challenges of we need to keep balancing security and convenience too. If* sistem keselamatan terlalu membebankan pelanggan susah juga … dah menghalang pelanggan daripada kemudahan penggunaan perkhidmatan bank tu".

Rajah 13: Contoh naratif informan

c) Ancaman Dalaman

Cabaran lain yang turut menjadi perhatian ialah ancaman daripada dalam organisasi itu sendiri. Walaupun sering kali perhatian diberikan kepada ancaman luaran seperti penggodam dan penipu, hakikatnya pekerja dalaman juga boleh menjadi pencetus kepada isu keselamatan siber sama ada secara sengaja mahupun tidak sengaja. Tindakan seperti menyalahgunakan akses, mendedahkan maklumat sulit atau gagal mematuhi protokol keselamatan boleh membuka ruang kepada pencerobohan siber. Informan turut mengakui bahawa bank juga perlu berusaha melindungi sistem mereka daripada ancaman dalaman yang boleh berlaku melalui pekerja tetap, kontraktor atau vendor dengan akses khas.

Isu ini menjadi sensitif kerana melibatkan kepercayaan antara organisasi dan pekerjanya. Dalam organisasi yang besar, tidak semua tindakan pekerja dapat diawasi secara terperinci, apatah lagi apabila mereka mempunyai autoriti tertentu dalam sistem kewangan. Kebocoran data yang berpunca daripada dalam boleh menyebabkan kerugian yang besar bukan sahaja dari segi kewangan, malah reputasi bank juga boleh tercalar. Tambahan pula, menguruskan ancaman dalaman memerlukan pendekatan yang berhati-hati dan sistematik. Ini termasuk pelaksanaan sistem pemantauan dalaman, kawalan akses yang ketat serta latihan berterusan kepada kakitangan mengenai etika kerja dan tanggungjawab keselamatan maklumat. Pengukuhan budaya integriti dalam kalangan pekerja juga amat penting bagi memastikan mereka sedar bahawa sebarang kecuaian atau tindakan sabotaj bukan sahaja menjejaskan organisasi tetapi turut membahayakan keselamatan pengguna dan kestabilan sistem kewangan negara. Hal ini dibukti oleh kenyataan informan dalam Rajah 14.

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4201-15

Naratif #TM5

"*Protecting against insiders … where banks must also protect against insider threats* contohnya, *employees or contractors with authorized access to financial information* secara sengaja atau tidak sengaja or *misuse it*".

Rajah 14: Contoh naratif informan

KESIMPULAN

Kajian ini telah memperlihatkan bagaimana pengurusan keselamatan siber dalam perbankan internet di Malaysia dilaksanakan melalui gabungan langkah teknikal dan amalan komunikasi risiko oleh institusi perbankan. Analisis dapatan menunjukkan bahawa kerentanan keselamatan tidak boleh ditafsirkan sebagai kegagalan sistem semata-mata, sebaliknya berpunca daripada hubungan saling mempengaruhi antara kelemahan teknologi, tahap literasi digital yang tidak seimbang serta corak tingkah laku dan kecuaian pengguna, di samping keterhadapan strategi komunikasi keselamatan. Walaupun pelbagai inisiatif perlindungan teknikal dan tindakan susulan seperti pembekuan akaun telah dilaksanakan, penekanan yang berlebihan terhadap aspek teknologi masih belum mampu menyediakan perlindungan menyeluruh terhadap ancaman siber yang semakin berkembang. Dari sudut pengurusan pula, kajian ini mendapati bahawa institusi perbankan memainkan peranan penting sebagai pengurus risiko siber, namun pelaksanaan strategi keselamatan masih bersifat reaktif dan kurang berfokus kepada dimensi komunikasi serta tingkah laku pengguna. Kebergantungan kepada penyampaian mesej keselamatan melalui laman sesawang rasmi dan amaran umum didapati tidak selari dengan corak penggunaan perbankan internet yang semakin tertumpu kepada aplikasi mudah alih. Keadaan ini telah melemahkan keberkesanan komunikasi risiko dan sekali gus menjejaskan tahap kesedaran, kepercayaan dan perlindungan pengguna terhadap sistem perbankan digital.

Selain daripada itu, secara konseptualnya, kajian ini menyumbang kepada bidang komunikasi dengan menegaskan bahawa keselamatan siber perbankan internet perlu difahami sebagai isu komunikasi risiko dan pengurusan tingkah laku, bukan semata-mata masalah teknikal. Pendekatan keselamatan yang berkesan memerlukan integrasi antara teknologi, komunikasi strategik dan pendidikan pengguna secara berterusan. Oleh itu, institusi perbankan disarankan untuk memperkukuh strategi komunikasi risiko melalui saluran yang lebih relevan dengan amalan penggunaan harian pengguna, di samping meningkatkan ketelusan dan akauntabiliti institusi dalam menangani insiden keselamatan siber. Selain itu, pihak perbankan dan pembuat dasar perlu mempertimbangkan pembangunan kerangka pengurusan keselamatan siber yang lebih holistik, proaktif dan berorientasikan pengguna. Kerangka ini perlu menggabungkan aspek perlindungan teknologi dengan strategi komunikasi risiko yang jelas, konsisten dan mudah difahami bagi meningkatkan daya tahan pengguna terhadap ancaman siber. Pada masa yang sama, usaha meningkatkan literasi digital masyarakat perlu dijadikan sebahagian daripada strategi keselamatan perbankan jangka panjang. Walaupun kajian ini memberi gambaran mendalam tentang pengurusan keselamatan siber perbankan internet di Malaysia, ia terhad kepada perspektif institusi perbankan terpilih dan pendekatan kualitatif. Kajian masa hadapan dicadangkan untuk melibatkan perspektif pengguna secara lebih meluas serta mengintegrasikan pendekatan kuantitatif bagi mengukuhkan pemahaman tentang hubungan antara komunikasi risiko, tingkah laku pengguna dan keberkesanan keselamatan siber dalam perbankan digital.

BIODATA

Muhammad Adnan Pitchan merupakan Pensyarah Kanan di Pusat Kajian Media dan Komunikasi, Fakulti Sains Sosial dan Kemanusiaan, UKM. Bidang kajian beliau adalah media baharu, undang-undang siber, dasar keselamatan siber serta kesejatheraan siber. E-mel: adnan86@ukm.edu.my

Nur Izzah 'Atirah Abdul Rahim merupakan pelajar di Pusat Kajian Media dan Komunikasi, Universiti Kebangsaan Malaysia. Bidang kajian beliau ialah komunikasi dan perbankan Internet. E-mel: atirahrahim1198@gmail.com

Siti Nur Husna Abd Rahman merupakan pensyarah di Universiti Teknologi MARA (UiTM), Malaysia. Bidang kajian beliau merangkumi pengurusan organisasi, komunikasi risiko, tadbir urus dan pembangunan model dalam konteks pengurusan kontemporari. E-mel: snhusna@uitm.edu.my

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2026-4201-15

RUJUKAN

Al-Doghan, M. A., & Mirzaliev, S. (2024). Cybersecurity awareness and digital bankin adoption: Exploring the moderating impact of digital literacy. *International Journal of Economics and Financial Studies, 16*(3), 34-58.

Arif, M., & Masdupi, E. (2020). Pengaruh Internet banking terhadap kinerja perbankan. *EcoGen*, *3*(4), 598-614.

Azura, Y. T. Y., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber securityrisk management framework for online banking systems. *Journal of Banking and Financial Technology, 9*, 85-104.

Bank Negara Malaysia. (2020). Financial stability review – First half 2020. https://www.bnm.gov.my/publications/fsr

Bank Negara Malaysia. (2021). Key indicators of financial inclusion. https://www.bnm.gov.my/financial-inclusion

CyberSecurity Malaysia. (2025). SR-031.082025: MyCERT Report - Cyber Incident Quarterly Summary Report - Q2 2025. https://www.mycert.org.my/portal/advisory?id=SR-031.082025

Hassan, S., Bujang, I., Othman, N. A. F., & Jati, M. K. (2025). From login to loyalty: The mediating role of trust in digital banking readoption. *Journal of Emerging Economies & Islamic Research, 13*(2), 4589.

INTERPOL. (2020). *ASEAN Cyberthreat Assessment 2020: Key Insights from the ASEAN Cybercrime Operations Desk*. https://share.google/ZCdeNNgPSsOCFAXRk

Jafri, J. A., Mohd Amin, S. I., Rahman, A., & Mohd Nor, S. (2023). A systematic literature review of the role of trust and security on FinTech adoption in banking. *Heliyon, 10*(1), e22980.

Lim, K. E., Pang, Y. H., Ooi, S. Y., Kow, W. X., Cheang, T. X., & Tan, M. W. (2025). Exploring user perceptions of security in mobile banking: A study in Malaysia. *Journal of Informatics and Web Engineering*, *4*(2), 303–314.

Manoharan, S., Katuk, N., Hassan, S., & Ahmad, R. (2022). To click or not to click the link: The factors influencing internet banking users' intention in responding to phishing emails. *Information & Computer Security*, *30*(1), 37–62.

Mohd Fuad@Mohd Daud, N. S., & Mohd Yusof, A. R. (2022). Memahami jenayah siber dan keselamatan siber di Malaysia: Suatu pemerhatian terhadap pandangan sarjana dan intelektual. *Asian Journal of Environment, History and Heritage*, *6*(1), 11-26.

Muhammad, M. Z., Muhamad, F. H., Doktoralina, C. M., Mukhtar, D., Ghazali, M. F., & Rahman, M. K. (2021). Internet banking of Islamic banks: Issues of security and privacy. *Society 5.0 Conferences, 11*, 142-156. https://doi.org/qxss

Nie Ching. (2023). Kes jenayah dalam talian bagi tempoh Jan–Sept meningkat 23 peratus. *ASTRO Awani*. https://www.astroawani.com/berita-malaysia/kes-jenayah-dalam-talian-bagi-tempoh-jansept-meningkat-23-peratus-nie-ching-445987

Waliullah, M., George, M. Z. H., Hasan, M. T., Alam, M. K., Munira, M. S. K., & Siddiqui, N. A. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(1), 226–257.

Wei, N., Lian, Y., Wang, H. & Liu, M. (2025). Analysis of mobile fintech adoption based on perceived value and risk factors. *Humanities and Social Sciences Communications*, *12*, 973.