INTERNATIONAL JOURNAL OF SOCIAL AND MANAGEMENT STUDIES (IJOSMAS)

Vol. 6 No. 4 (2025): August 2025 https://www.ijosmas.org e-ISSN: 2775-0809

Pengaruh Cybercrime Knowledge dan Cybercrime Security Terhadap Loyalitas Pengguna Internet e-banking

Yohanes Prasetya Husada
Universitas Brawijaya
free2fly357@gmail.com

Abstrak
Tujuan penelitian ini adalah menganalisis hubungan antara pengetahuan kejahatan siber dengan loyalitas nasabah bank dan menguji hubungan antara keamanan kejahatan siber dengan loyalitas nasabah bank. Desain penelitian yang digunakan dalam penelitian ini adalah desain penelitian metode survei kuantitatif. Teknik yang digunakan dalam pemilihan sampel dalam penelitian ini adalah simple random sampling. Pengumpulan data dalam penelitian ini dilakukan secara daring dengan menyebarkan kuesioner melalui platform Google Form dan memperoleh tanggapan langsung dari responden. Jumlah responden yang diteliti sebanyak 621 nasabah Bank di Indonesia yang sering menggunakan Internet banking. Teknik Analisis Data Penelitian ini menggunakan teknik analisis jalur dalam melakukan pengujian data dan hipotesis. Pengujian statistik pada model analisis jalur dapat dilakukan dengan menggunakan metode partial least square. Penelitian ini menggunakan skala likert yang dikategorikan menjadi lima kategori, meliputi: (1) sangat tidak setuju, (2) tidak setuju, (3) netral, (4) setuju dan (5) sangat setuju. Analisis data dalam penelitian ini menggunakan perangkat lunak Smart Partial Least Square (SPLS) versi 3.00. Evaluasi model dalam pengujian dengan SPLS terdiri dari dua tahap yaitu, evaluasi outer model dan inner model. Evaluasi model luar terdiri dari uji pemuatan faktor, Average Variance Extracted, pemuatan silang, alpha Cronbach, dan reliabilitas komposit, sedangkan evaluasi model dalam terdiri dari koefisien determinasi (R2), redundansi tervalidasi silang (Q2), Goodness of Fit (GoF), dan pengujian hipotesis. Setelah melakukan beberapa langkah penelitian dan pengolahan data yang diperlukan dalam penelitian ini, beberapa kesimpulan dapat ditarik, yaitu hasil uji hipotesis korelasi pertama menunjukkan bahwa pengetahuan tentang kejahatan siber berpengaruh signifikan terhadap loyalitas nasabah, dapat juga diartikan bahwa pengetahuan nasabah berpengaruh terhadap loyalitas nasabah. Hasil uji hipotesis korelasi kedua menunjukkan bahwa keamanan kejahatan siber berpengaruh positif dan signifikan terhadap loyalitas nasabah, dapat juga diartikan bahwa keamanan nasabah berpengaruh terhadap loyalitas nasabah.

Kata Kunci: Pengetahuan tentang kejahatan siber, Keamanan kejahatan siber, Loyalitas nasabah e-banking.Bank Indonesia

1. Pendahuluan

Vol. 6 No. 4 (2025): August 2025 https://www.ijosmas.org e-ISSN: 2775-0809

Di era revolusi industri dan digital 5.0, salah satu perkembangan yang sangat pesat saat ini adalah perkembangan di bidang teknologi informasi, yang diterapkan dalam dunia perbankan, termasuk Internet banking. Internet Banking saat ini bukan lagi istilah yang asing bagi masyarakat Indonesia, hal ini disebabkan oleh banyaknya bank-bank nasional yang menggunakan layanan Internet banking, Internet atau yang disebut juga Cyberspace, yang dapat diartikan sebagai ruang tempat entitas elektronik (netter) berinteraksi [1]. Sifat aktivitas internet yang unik dan tidak mengenal batas teritorial negara pada akhirnya menimbulkan permasalahan mendasar, yaitu mengenai kemampuan hukum untuk menjalankan fungsinya mengatur dan menegakkan sanksi serta bagaimana kemampuan bank untuk melindungi nasabah bank. Namun, kehadiran internet sama sekali tidak dapat dihindari dalam sejarah perkembangan peradaban manusia. Kehadirannya merupakan bagian dari sejarah perkembangan pemikiran manusia, teknologi, dan ilmu pengetahuan itu sendiri. Perkembangan internet semakin hari semakin meningkat, baik secara teknologi maupun penggunaannya, membawa banyak dampak positif dan negatif. Bagi yang positif karena banyaknya manfaat dan kemudahan yang diperoleh dari teknologi ini, misalnya, kita dapat melakukan transaksi perbankan kapan saja dan di mana saja dengan menggunakan fasilitas internet banking[2].

Perkembangan teknologi informasi dan digitalisasi berdampak pada pergeseran perilaku masyarakat yang lebih berorientasi pada mobilitas dan fleksibilitas. Pertumbuhan transaksi digital global juga meningkat pesat. Jumlah pengguna internet dan koneksi seluler yang terus meningkat, menandakan masyarakat Indonesia sangat terbuka terhadap tren digitalisasi yang sedang berkembang saat ini. Teknologi kini telah menjadi kebutuhan bagi setiap individu, baik teknologi informasi maupun teknologi masyarakat. Kemajuan teknologi berkembang sangat pesat, sehingga mempengaruhi naik turunnya minat pasar terhadap sektor perbankan. Kemajuan teknologi yang mendukung kemudahan layanan perbankan menyebabkan persaingan antarbank yang semakin ketat, untuk menjaga loyalitas nasabah[3]. Salah satu faktor penting yang memengaruhi masyarakat dalam menggunakan teknologi internet adalah kepercayaan. Kepercayaan merupakan fondasi bagi keberhasilan hubungan dan loyalitas dengan nasabah. Keamanan menjadi salah satu alasan utama keterlambatan dalam pengembangan layanan berbasis teknologi. Keamanan inilah yang dapat mencegah terjadinya penipuan dari suatu sistem berbasis informasi. Kebocoran data pribadi membuat sebagian kecil masyarakat masih meragukan pemanfaatan teknologi informasi. Namun, tuntutan persaingan di dunia perbankan juga turut membangun fasilitas serupa[4].

Adaptasi terhadap teknologi menjadi tantangan terbesar bagi industri perbankan karena beberapa risiko akan menjadi momok yang sangat menakutkan. Lagipula, semakin berkembangnya teknologi, maka akan semakin banyak pula ancaman yang datang dari waktu ke waktu. Layanan Mobile Banking diciptakan agar nasabah dapat lebih mudah melakukan transaksi perbankan

syariah[5]. Namun, nasabah harus berhati-hati karena layanan perbankan ini rentan terhadap risiko. Risiko yang ditimbulkan oleh operasional bank maupun kelalaian nasabah, risiko yang dialami oleh Mobile Banking adalah Cyber Crime. Cybercrime adalah setiap tindakan yang dilakukan secara langsung maupun tidak langsung melalui komputer dan jaringan komputer (internet) yang melanggar etika, hukum, dan kewenangan terkait dengan pemrosesan data dan penyampaian data. Ancaman Cybercrime terhadap keamanan dan kepercayaan nasabah dalam menggunakan jasa dalam pemanfaatan layanan teknologi perbankan di Indonesia sudah sangat besar, perbankan harus berlomba-lomba untuk memenangkan persaingan dalam menjaring minat nasabah[6]. Penggunaan internet banking dapat mempengaruhi perlindungan data nasabah, dan penggunaan internet banking berdampak besar terhadap peningkatan cybercrime. Lemahnya keamanan pada fitur internet banking dapat memudahkan oknum untuk melakukan tindak kejahatan yang merugikan nasabah. Untuk tindakan kriminal, terutama pada produk perbankan internet di bank syariah, bank harus menyediakan fitur keamanan yang dapat menjaga kepercayaan nasabah untuk bertransaksi menggunakan elektronik. Dampak kejahatan siber pada sektor perbankan berkembang sangat pesat karena dengan perangkat seluler dengan konektivitas internet. Kejahatan tersebut biasanya dengan menggunakan identitas alamat IP nasabah[7]. Kejahatan siber di perbankan, terutama di Indonesia, sering menjadi tajuk utama dalam berbagai berita perbankan dalam beberapa tahun terakhir. Kejahatan siber ini memiliki pengaruh besar pada loyalitas nasabah karena kepuasan dan ketidakpuasan nasabah terlihat dalam layanan di bank syariah. Penggunaan perbankan internet memiliki pengaruh besar pada kejahatan siber untuk perlindungan nasabah bank. Dampak kejahatan siber mencakup pengalaman, keamanan, dan pengetahuan. Hal ini merujuk pada sebuah penelitian yang juga meneliti dampak kejahatan siber terhadap loyalitas nasabah pengguna produk E-Banking. Pentingnya keamanan perbankan seluler dalam memengaruhi kepuasan nasabah disebabkan oleh keinginan setiap bank agar nasabah merasa puas dengan layanan yang diberikan oleh bank[8].

Keamanan di bank tidak ditentukan oleh sistem otomatis di back end atau di balik layar suatu sistem, melainkan oleh perilaku pengguna atau nasabah. Banyak bank yang mengembangkan keamanan terpadu dengan menggunakan teknologi kecerdasan buatan. Sistem keamanan yang paling canggih dari segi integritas saja tidak cukup untuk mencegah serangan siber [9]. Risiko penyebaran yang diterima oleh bank disebabkan oleh banyaknya kejahatan yang disebabkan oleh jaringan internet, sehingga menurunkan tingkat kepercayaan dan loyalitas nasabah. Nasabah merasa tidak puas dengan kualitas dan keamanan yang diterima dari penggunaan Mobile Banking. Penggunaan mobile banking tidak lepas dari berbagai tindakan kejahatan siber yang menjadi masalah bagi pengguna mobile banking, kejahatan berupa phishing dengan mencuri data identitas nasabah seperti user ID, password, hingga pin yang kemudian dikendalikan oleh orang lain yang digunakan untuk mengakses rekening koran bank, dan masih banyak lagi modus kejahatan siber lainnya. Dampaknya adalah menurunnya minat nasabah dalam menggunakan layanan Mobile Banking yang disediakan oleh bank syariah. Bank syariah Indonesia harus

melakukan evaluasi dan memperbaiki segala kekurangan yang terjadi untuk memberikan kepuasan nasabah dan menjaga loyalitas nasabah dalam menggunakan Mobile Banking.

.

Dalam dunia perbankan terdapat berbagai layanan transaksi seperti penyetoran, penarikan, transfer, kliring dan lain sebagainya. Semua transaksi tersebut masih banyak dilakukan oleh nasabah bank pada bank yang bersangkutan. Sehingga ketika nasabah bank sedang sibuk melakukan transaksi perbankan, nasabah yang lain terpaksa harus antri untuk dilayani oleh pihak bank. Hal ini menjadi permasalahan bagi nasabah bank karena nasabah bank membuang-buang waktu mereka untuk menunggu dalam antrian dan hal ini juga berdampak pada pihak bank itu sendiri karena pihak bank harus menyediakan unit layanan yang lebih banyak seperti counter teller harus ditambah, ruangan, kursi dan lain sebagainya sehingga menimbulkan biaya yang cukup besar[10]. Kemudian perkembangan teknologi dan informasi saat ini sangat pesat, begitu pula pada dunia perbankan. Dunia perbankan seakan tidak mau ketinggalan dengan kemajuan teknologi dan informasi[11]. Buktinya perbankan saat ini tengah mengembangkan layanan perbankan yang selaras dengan kemajuan teknologi dan informasi. Sebagai contoh, dunia perbankan telah mengeluarkan layanan yang bernama Electronic Banking (E-Banking). E-banking merupakan layanan perbankan yang dilakukan secara elektronik. Jenis layanan E-Banking secara umum meliputi Kartu ATM/Debit, Kartu Kredit, Tele Banking/Phone Banking, SMS Banking, Mobile Banking dan Internet Banking. Nasabah bank saat ini sudah banyak menggunakan ATM atau Kartu Debit, hal ini dikarenakan pada umumnya bank memiliki keterbatasan penarikan tunai, jika menarik uang di bawah lima juta rupiah harus melalui ATM. Sedangkan Kartu Kredit banyak digunakan oleh kalangan tertentu karena tidak semua nasabah bank berminat menggunakannya.

Tele Banking/Phone Banking, SMS Banking, Mobile Banking dan Internet Banking, tidak semua nasabah bank menggunakan layanan tersebut, hanya kalangan tertentu saja yang menggunakannya terutama para pebisnis. Hal ini dibuktikan dengan masih panjangnya antrian di beberapa bank dan ATM saat melakukan transaksi perbankan. Saat ini penggunaan Internet dapat dikatakan semakin baik, karena hampir setiap orang yang menggunakan perangkat komunikasi dapat terhubung dengan Internet. Otomatis setiap orang yang terhubung dengan Internet dapat melakukan transaksi secara online, hal ini tergantung dari kemauan individu dan jenis transaksi online apa yang dibutuhkan oleh pengguna Internet[12]. Jika dikaitkan dengan nasabah bank, kemungkinan besar rata-rata nasabah bank sudah menggunakan perangkat komunikasi atau perangkat lain yang dapat terhubung ke Internet. Sehingga dapat menggunakan fasilitas Internet untuk melakukan transaksi perbankan secara online, yaitu menggunakan layanan Internet Banking. Namun ketika menggunakan Internet Banking, apakah aman? Karena ketika menggunakan Internet, perangkat komunikasi atau perangkat komputer terhubung ke jaringan global, sehingga sangat rentan terhadap serangan keamanan Internet Banking. Untuk itu, makalah ini akan membahas keamanan layanan Internet Banking dalam transaksi perbankan.

Tujuan dari penelitian ini adalah untuk menganalisis hubungan antara pengetahuan kejahatan siber dan loyalitas nasabah bank dan untuk menguji hubungan antara keamanan kejahatan siber dan loyalitas nasabah bank.

2. Literature Review

2.1. Kejahatan Siber

Kejahatan siber merupakan kejahatan yang berkaitan dengan komputer atau perangkat jaringan, biasanya kejahatan ini dilakukan secara daring. Kejahatan siber ini pun dapat menyasar siapa saja, Jika menjadi salah satu korbannya tentu saja akan mengakibatkan banyak kerugian, Kejahatan siber dalam arti luas merupakan kejahatan yang menyangkut sistem atau jaringan komputer dan kejahatan yang menggunakan sarana komputer[13]. Sedangkan kejahatan siber dalam arti sempit diartikan hanya sebagai kejahatan sistem komputer. Kejahatan siber merupakan tindakan kriminal yang memanfaatkan teknologi, mulai dari perangkat hingga jaringan internet. Tujuan dari kasus kejahatan siber adalah merugikan orang lain dengan melakukan pencurian, peretasan, penipuan, penyebaran virus, dan kejahatan digital lainnya. Di era perkembangan teknologi, kasus kejahatan siber semakin marak di seluruh dunia dan jenis kejahatannya pun beragam. Kemajuan teknologi yang semakin pesat diiringi dengan sistem keamanan yang semakin pesat sebagai respon terhadap meningkatnya kejahatan siber. Akibatnya, para pelaku kejahatan siber selalu lebih aktif dan cepat melakukan terobosan dalam sistem keamanan yang telah dibentuk oleh kejahatan siber[14]. Kondisi ini sangat mengkhawatirkan bagi para pelaku kejahatan siber sehingga modus-modus baru sulit dideteksi dan dipecahkan dengan keamanan siber. Kejahatan siber merupakan kejahatan yang terjadi di dunia maya atau internet. Setiap tahunnya kejahatan ini cenderung meningkat, baik dari jumlah kasusnya maupun ragam serangannya yang semakin maju seiring dengan perkembangan teknologi internet itu sendiri. Oleh karena itu, bermunculanlah kejahatan-kejahatan baru di dunia internet atau new cybercrime. Arti sempit dari kejahatan siber adalah kejahatan komputer yang ditunjukkan pada suatu sistem atau jaringan, sedangkan arti luas kejahatan siber mencakup segala bentuk kejahatan yang ditunjukkan pada komputer, jaringan komputer dan penggunaannya serta bentuk-bentuk kejahatan tradisional yang kini dilakukan dengan bantuan perangkat komputer. Bentuk Kejahatan Siber yang sering digunakan oleh para pelaku adalah email spoofing, yaitu pemalsuan header email. Pesan dalam email yang diterima seolah-olah dikirim oleh sumber yang asli, sebenarnya, dan terpercaya. Penyebaran virus merupakan sekumpulan instruksi siber yang mampu melakukan beberapa operasi jahat. Virus ini menghentikan fungsi normal program sistem dan menyisipkan beberapa kelainan pada kinerja sistem yang diserang yang dapat menyebar melalui email, pesan, obrolan, penyimpanan data, multimedia, internet, dan media elektronik lainnya (Anggono & Riskiyadi, 2021). Kerugian akibat kejahatan siber sulit diperkirakan dan diverifikasi karena, selain kerugian finansial, kerugian lain akibat kerusakan, kehilangan, atau kebocoran data pribadi menyebabkan penurunan reputasi perusahaan. Untuk mempelajari tindakan kriminal ini, diperlukan kriminologi siber,

yang merupakan gabungan pengetahuan dari kriminologi, psikologi, sosiologi, ilmu komputer, dan keamanan siber untuk memberikan pemahaman yang mendalam tentang kejahatan siber[15].

Kejahatan siber yang sering dikenal dengan cybercrime merupakan tindakan kriminal yang berbasis pada komputer dan jaringan internet. Pelaku kejahatan siber biasanya meretas sistem untuk mendapatkan data pribadi korban. Terdapat berbagai jenis kejahatan siber. Berikut adalah empat jenis kejahatan siber: Phishing dan Penipuan. Sesuai namanya, phishing dapat diartikan sebagai pelaku yang "memancing" korban untuk memberikan identitas dan informasi pribadi mereka. Banyak orang tidak menyadari bahwa dirinya sedang terkena penipuan phishing karena pelaku pandai berbicara dengan "memancing" korban dengan pertanyaan jebakan[16]. Peretasan, Peretasan merupakan suatu usaha untuk menyusup ke dalam sistem komputer tanpa izin. Beberapa hal yang biasa dilakukan oleh peretas adalah membobol sistem, dan mencuri data pribadi serta data keuangan. Cyber Stalking atau Penguntit Siber adalah pemanfaatan internet dan teknologi lainnya untuk menguntit atau meneror korban. Penguntit akan melakukan sesuatu secara berulang-ulang. Selain membuat korban merasa terganggu, perilaku penguntit juga dapat membahayakan nyawa korban. Perundungan siber merupakan perundungan atau penindasan yang dilakukan secara daring melalui internet dan teknologi lainnya. Biasanya, hal ini terjadi pada kolom komentar di berbagai media sosial. Kejahatan siber semakin marak[17]. Hal ini tidak terlepas dari perkembangan teknologi digital yang memberikan kemudahan dalam bertransaksi hingga berbelanja hanya dengan akses internet. Namun, perkembangan teknologi ini juga dimanfaatkan oleh orang-orang yang tidak bertanggung jawab untuk melakukan berbagai modus kejahatan yang mengandalkan jaringan internet atau biasa disebut dengan kejahatan siber. Kejahatan siber adalah kejahatan di dunia maya yang memanfaatkan teknologi komputer dan jaringan internet untuk mencuri data seseorang demi keuntungan pribadi. Kejahatan siber dapat menimbulkan kerugian materiil dan non-materiil bagi korbannya. Umumnya, pengguna internet masih kurang menyadari betapa pentingnya keamanan data pribadi yang seharusnya bersifat rahasia. Informasi yang terkesan sepele seperti nomor ponsel, lokasi, media sosial, dan tanda tangan dapat menjadi target pelaku kejahatan siber untuk melancarkan aksinya.[18]

2.1. Internet Banking

Internet Banking merupakan kegiatan perbankan yang memanfaatkan teknologi internet sebagai media untuk melakukan transaksi dan memperoleh informasi lainnya melalui situs web bank. Kegiatan ini memanfaatkan jaringan internet sebagai perantara atau penghubung antara nasabah dengan bank tanpa harus mengunjungi kantor bank.[19]. Internet banking atau yang dikenal juga dengan e-banking merupakan layanan yang digunakan untuk melakukan berbagai transaksi keuangan pada situs web resmi bank melalui peramban (browser). Situs web tersebut dapat diakses apabila nasabah memiliki koneksi internet dan telah terdaftar pada layanan ini. Internet banking merupakan layanan bank yang memanfaatkan kecerdasan teknologi di mana nasabah dapat melakukan transaksi melalui internet seluler. [20] Layanan ini tentunya sangat

Vol. 6 No. 4 (2025): August 2025 https://www.ijosmas.org e-ISSN: 2775-0809

memudahkan nasabah bank saat ini, mereka tidak perlu lagi pergi ke bank atau ATM ketika ingin bertransaksi. Industri perbankan di Indonesia mengikuti pola perkembangan teknologi yang sama seperti yang diadopsi oleh bank-bank di negara-negara maju. Dengan berkembangnya teknologi perbankan ini, sistem di bank, khususnya back office, berkaitan dengan fungsi keuangan dan administrasi yang dikelola pada rekening nasabah. Internet banking merupakan pengembangan dari perbankan elektronik yang memungkinkan adanya integrasi antara fungsi operasional dan pemasaran dalam melayani nasabah. Internet banking dapat menjadi salah satu fasilitas platform standar dalam hal layanan perbankan di Indonesia dan akan terus dikembangkan di masa mendatang. Internet banking merupakan salah satu penyedia layanan yang disediakan oleh bank yang memanfaatkan jaringan internet yang memungkinkan nasabah memperoleh layanan dan jasa perbankan seperti informasi dan melakukan transaksi perbankan dengan mudah[21].

Internet Banking merupakan layanan pada bank yang memungkinkan nasabah memperoleh informasi, berkomunikasi dan melakukan transaksi perbankan dengan menggunakan jaringan internet, tidak hanya menyediakan layanan melalui internet. Secara umum, penyediaan layanan internet banking memberikan informasi mengenai produk dan layanan melalui portal web internet, serta memberikan akses kepada nasabah untuk bertransaksi dan memperbarui data pribadi lainnya. Fitur pada layanan internet banking dapat dilakukan melalui layanan seperti: pengecekan informasi saldo, mutasi rekening, dan transfer online. Aktivitas perbankan ini tidak lagi menggunakan aplikasi berupa slip yang diisi langsung oleh nasabah di bank[23]. Perbankan dapat diakses dengan menggunakan electronic banking, bank menjadi semakin berkurang. Namun, ada fasilitas perbankan elektronik yang disediakan oleh bank yang sangat membantu nasabah dalam melakukan transaksi tanpa dibatasi oleh ruang dan waktu. Jenis-jenis kegiatan internet banking dibagi menjadi tiga jenis, yaitu: Setiap fasilitas yang disediakan oleh suatu produk atau layanan selalu memiliki kelebihan dan kekurangan. Begitu pula dengan layanan Internet Banking yang memiliki kelebihan dan kekurangan. a. Kelebihan: 1) Memudahkan nasabah dalam melakukan aktivitas perbankan tanpa harus pergi ke bank kecuali untuk setoran tunai atau penarikan tunai. 2) Aktivitas perbankan dapat dilakukan kapan saja dan di mana saja selama ada akses internet. 3) Memudahkan nasabah untuk membawa uang tunai dalam jumlah besar ketika melakukan transfer. Sehingga dapat melindungi nasabah dari perampokan. 4) Memudahkan nasabah untuk membayar tagihan tanpa harus datang ke lokasi pembayaran tagihan. 5) Memudahkan nasabah untuk melakukan pembelian tiket dan kredit tanpa harus datang ke loket penjualan tiket dan kredit. 6) Keamanan sistem Internet Banking berlapis, mulai dari user ID dan password, kemudian website menggunakan SSL dengan algoritma berlapis dan adanya autentikasi kedua untuk verifikasi transaksi seperti token atau keycode[24].

E-banking adalah penyampaian layanan dan produk bank secara otomatis langsung kepada nasabah melalui media elektronik dan saluran komunikasi interaktif. E-banking adalah sistem yang memungkinkan nasabah bank, baik perorangan maupun bisnis, untuk mengakses rekening,

melakukan transaksi bisnis, atau memperoleh informasi produk dan layanan bank melalui jaringan privat atau publik, termasuk Internet. Internet banking adalah layanan perbankan yang menggunakan kecerdasan teknologi di mana sebagian nasabah dapat melakukan transaksi secara mobile berbasis internet. Layanan ini tentunya telah memudahkan sebagian nasabah bank saat ini, mereka tidak perlu pergi ke bank atau ATM ketika ingin bertransaksi. Internet banking merupakan hasil dari fintech di era yang semakin canggih ini[25]. Dalam menggunakannya, perlu memiliki komputer atau ponsel dan tentunya jaringan internet. Saat ini, sebagian besar bank di Indonesia sudah memiliki layanan e-banking atau internet banking. Umumnya, ketika Anda mendaftar akun di bank, Anda akan langsung diarahkan untuk mendaftar internet banking. Definisi perbankan internet dan fitur-fiturnya mencakup informasi umum mengenai akun Anda (termasuk giro dan setoran), saldo, mutasi, transfer dana antar bank atau rekening, pembelian utilitas seperti kredit, listrik, telepon, internet, dan lainnya.

2.1. Loyalitas Pelanggan

Loyalitas pelanggan adalah komitmen yang dipegang erat oleh pelanggan dalam membeli atau mengutamakan suatu produk atau jasa secara terus-menerus. Loyalitas dapat disimpulkan sebagai komitmen pelanggan terhadap suatu produk berdasarkan kegunaannya. Dapat diartikan sebagai kesetiaan, yaitu kesetiaan seseorang terhadap suatu objek. Pelanggan adalah seseorang yang terbiasa membeli suatu produk[26]. Pelanggan adalah seseorang yang terbiasa membeli suatu produk. Dengan kebiasaan yang terbentuk melalui pembelian dan interaksi yang sering dalam periode tertentu. Loyalitas adalah kesediaan pelanggan untuk tetap setia dengan menggunakan produk suatu perusahaan dalam jangka panjang. Loyalitas pelanggan adalah komitmen pelanggan terhadap suatu produk atau jasa yang positif dalam pembelian jangka panjang. Dalam pengertian ini, dapat diartikan bahwa kesetiaan terhadap suatu merek diperoleh karena adanya kombinasi antara kepuasan pelanggan dan keluhan. Pelanggan yang loyal adalah pelanggan yang merasa puas terhadap produk dan jasa tertentu. Loyalitas merek atau loyalitas pelanggan merupakan dua istilah yang hampir serupa maknanya, oleh karena itu keduanya sering disebut sebagai loyalitas merek. Seseorang dikatakan sebagai pelanggan apabila orang tersebut mulai terbiasa membeli produk atau jasa yang ditawarkan oleh badan usaha tersebut[27]. Loyalitas pelanggan merupakan suatu kondisi yang diharapkan oleh setiap perusahaan, terutama perusahaan jasa seperti perbankan. Loyalitas pelanggan yang tinggi dapat mengindikasikan keberhasilan suatu perusahaan. Loyalitas pelanggan didefinisikan sebagai keinginan yang kuat dari pelanggan untuk melakukan pembelian ulang suatu produk atau layanan dan tidak berpindah ke perusahaan lain. Loyalitas pelanggan merupakan suatu kondisi yang diharapkan oleh setiap perusahaan, terutama pada perusahaan jasa seperti perbankan. Loyalitas pelanggan yang tinggi dapat mengindikasikan keberhasilan suatu perusahaan. Loyalitas pelanggan didefinisikan sebagai keinginan yang kuat dari pelanggan untuk melakukan pembelian ulang suatu produk atau layanan dan tidak berpindah ke perusahaan lain. Pelanggan yang loyal akan selalu melakukan pembelian ulang di masa mendatang jika membutuhkan produk atau layanan yang sama. Melihat

peran loyalitas pelanggan yang sangat krusial bagi perusahaan, banyak ahli yang meneliti kontribusi penting loyalitas pelanggan bagi perusahaan.

Loyalitas pelanggan merupakan komitmen yang dipegang erat oleh pelanggan dalam membeli atau mengutamakan suatu produk atau layanan secara terus menerus. Dapat disimpulkan bahwa loyalitas merupakan komitmen pelanggan terhadap suatu produk berdasarkan kegunaannya. Dari penjelasan tersebut, mencakup beberapa komponen penting, yaitu loyalitas pelanggan dan perilaku pelanggan [28]. Loyalitas sangat penting dalam menjaga perkembangan suatu perusahaan agar nasabah merasa sangat puas menggunakan produk dan layanan di perbankan, sehingga pihak bank harus mengambil langkah yang tepat dalam mempertahankan nasabah yang loyal. Dengan memiliki nasabah yang loyal tentunya akan mendapatkan banyak manfaat, misalnya nasabah tersebut tidak mudah berpindah ke produk pesaing dan nasabah tersebut memiliki inisiatif untuk memberikan rekomendasi penggunaan produk perbankan. b. Manfaat Loyalitas Nasabah Nasabah yang loyal merupakan aset penting dalam perusahaan. Nasabah yang puas tidak akan segan-segan menyebarkan hal-hal positif mengenai produk perbankan. Membangun dan mempertahankan loyalitas nasabah sebagai bagian dari program hubungan jangka panjang dengan perusahaan terbukti memberikan manfaat bagi nasabah.

2.4. Pengembangan Hipotesis

2.4.1. Hubungan antara Kejahatan Siber dan Loyalitas Nasabah Bank

Jika penanganan kejahatan siber dapat ditangani dengan baik oleh Bank, maka nasabah merasa aman dan akan loyal kepada bank[29]. Terdapat pengaruh langsung yang positif dan signifikan antara variabel Kejahatan Siber dan Kepercayaan Nasabah Bank. Jika penanganan kejahatan siber dapat ditangani dengan baik oleh Bank, maka nasabah merasa aman dan akan percaya kepada Bank. Terdapat pengaruh langsung yang positif dan signifikan antara variabel Kepercayaan dan Loyalitas Nasabah. Jika kepercayaan nasabah meningkat dalam bentuk penanganan kejahatan siber, maka nasabah akan loyal. Terdapat pengaruh tidak langsung yang positif dan signifikan antara variabel Kejahatan Siber dan Loyalitas Nasabah melalui Kepercayaan sebagai variabel intervening pada Nasabah Bank. Jika penanganan kejahatan siber dapat ditangani dengan baik oleh Bank, maka nasabah akan merasa loyal melalui kepercayaannya kepada Bank. Dampak yang ditimbulkan oleh kejahatan siber terhadap kepercayaan masyarakat dalam menggunakan layanan e-banking bersifat positif, namun tidak terlalu signifikan terhadap kepercayaan masyarakat dalam menggunakan layanan e-banking[30]. Nasabah terbantu dengan adanya e-banking karena memudahkan bertransaksi tanpa harus datang ke gerai bank. Makna dampak positifnya adalah nasabah tidak merasa khawatir akan ancaman kejahatan siber yang dilakukan oleh pihak-pihak yang bertanggung jawab atas pencurian data atau saldo rekening untuk keuntungan pribadi. Oleh karena itu, hal ini sangat memengaruhi kepercayaan pengguna layanan e-banking. Ketika keamanan suatu jaringan atau sistem terbebas

dari kejahatan, maka tingkat kepercayaan pengguna pun meningkat. Kejahatan siber ini berdampak signifikan terhadap pengguna e-banking, yaitu karena adanya fasilitas keamanan yang disediakan berupa password untuk login sehingga pengguna e-banking merasa aman saat menggunakannya. Berdasarkan penelitian ini, dirumuskan hipotesis sebagai berikut:
H1: Pengetahuan tentang kejahatan siber memiliki hubungan positif dan signifikan dengan loyalitas nasabah bank

2.4.2. Hubungan antara Keamanan Kejahatan Siber dan Loyalitas Nasabah Bank
Keamanan dalam kejahatan siber merupakan tindakan untuk melindungi informasi di dunia maya dari berbagai serangan. Kejahatan siber semakin marak karena semakin banyaknya penggunaan komputer seperti desktop, komputer, laptop, smartphone, server, dan perangkat lainnya[31]. Dari hasil penelitian, keamanan kejahatan siber menjadi topik utama penelitian. Di era teknologi dan informasi yang berkembang pesat, hal ini berdampak pada semua aspek kehidupan. Salah satunya adalah keamanan siber memiliki peran penting dalam mencegah kejahatan siber. Oleh karena itu, keamanan kejahatan siber berdampak pada loyalitas nasabah. Hasil penelitian ini juga dapat menunjukkan bahwa keamanan dapat memengaruhi kepercayaan nasabah dalam menggunakan internet banking[32]. Jika nasabah percaya, hal ini dapat membuat nasabah tetap loyal menggunakan produk dan layanan di bank syariah. Pencegahan kejahatan siber dapat dilakukan melalui pencegahan dan penegakan hukum. Jika dibiarkan, hal ini dapat mengganggu keamanan baik secara nasional maupun internasional. Kejahatan siber dilakukan dengan lebih menekankan pada serangan internet, oleh karena itu diperlukan pengalaman sistem untuk mencegahnya baik secara nasional maupun internasional. Faktor keamanan dalam penelitian ini memiliki pengaruh positif dan signifikan terhadap loyalitas nasabah. Objek penelitian ini memutuskan untuk tetap menggunakan layanan bank tersebut setelah tragedi kejahatan yang menyerang bank tersebut. Berdasarkan penelitian ini, hipotesis berikut dirumuskan:
H2: Keamanan kejahatan siber memiliki hubungan positif dan signifikan dengan loyalitas nasabah bank.

3. Metode Penelitian
Desain penelitian yang digunakan dalam penelitian ini adalah desain penelitian metode survei kuantitatif. Teknik yang digunakan dalam memilih sampel dalam penelitian ini adalah simple random sampling. Pengumpulan data dalam penelitian ini dilakukan secara daring dengan menyebarkan kuesioner melalui platform Google Form dan memperoleh tanggapan langsung dari responden. Jumlah responden yang diteliti adalah 621 nasabah Bank di Indonesia yang sering menggunakan Internet banking. Teknik Analisis Data Penelitian ini menggunakan teknik analisis jalur dalam melakukan data dan pengujian hipotesis. Pengujian statistik pada model analisis jalur dapat dilakukan dengan menggunakan metode partial least square. Penelitian ini menggunakan skala likert yang dikategorikan menjadi lima kategori, meliputi: (1) sangat tidak setuju, (2) tidak setuju, (3) netral, (4) setuju dan (5) sangat setuju. Analisis data dalam penelitian

ini menggunakan perangkat lunak Smart Partial Least Square (SPLS) versi 3.00. Evaluasi model dalam pengujian dengan SPLS terdiri dari dua tahap yaitu, evaluasi outer model dan inner model. Evaluasi model luar terdiri dari uji pemuatan faktor, Average Variance Extracted, pemuatan silang, alpha Cronbach, dan reliabilitas komposit, sedangkan evaluasi model dalam terdiri dari koefisien determinasi (R2), redundansi validasi silang (Q2), Goodness of Fit (GoF), dan pengujian hipotesis.

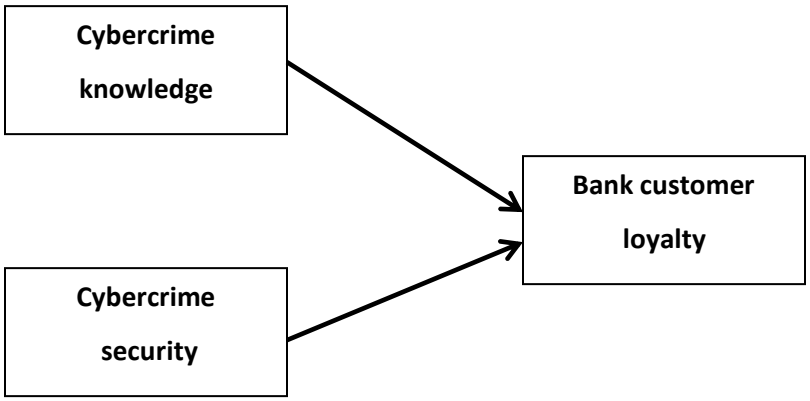


Fig 1. Research Model

Hipotesis penelitian ini adalah:

H1: Pengetahuan tentang kejahatan siber memiliki hubungan positif dan signifikan dengan loyalitas nasabah bank
H2: Keamanan kejahatan siber memiliki hubungan positif dan signifikan dengan loyalitas nasabah bank

3. Hasil dan Pembahasan

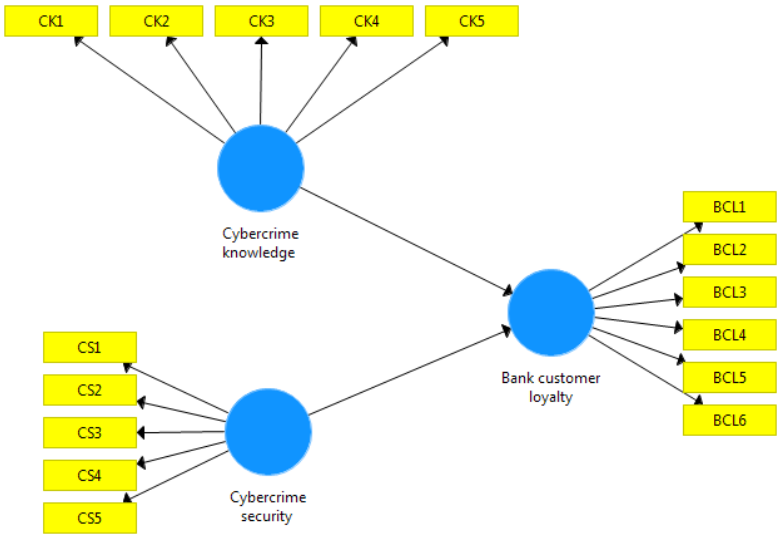
4.1. Karakteristik Responden

Jumlah responden yang diteliti adalah 621 nasabah Bank di Indonesia yang sering menggunakan internet banking di Indonesia. Karakteristik responden berdasarkan usia memiliki pilihan usia kurang dari 25 tahun, 25-50 tahun, dan lebih dari 50 tahun. Jumlah responden yang berusia kurang dari 25 tahun sebanyak 20%, responden berusia 25-50 tahun sebanyak 60%, dan yang berusia lebih dari 50 tahun sebanyak 30%. Karakteristik responden berdasarkan jenis kelamin memiliki pilihan jenis kelamin laki-laki dan perempuan, didapatkan jenis kelamin laki-laki sebanyak 65%, dan jenis kelamin perempuan sebanyak 35%. Karakteristik responden

berdasarkan tingkat pendidikan memiliki pilihan jenis kelamin SMA, diploma, sarjana, magister, dan doktoral, didapatkan tingkat pendidikan SMA sebanyak 15%, tingkat pendidikan diploma sebanyak 25%, tingkat pendidikan sarjana sebanyak 20%, tingkat pendidikan magister sebanyak 30%, dan tingkat pendidikan doktoral sebanyak 10%.

4.2. Uji Validitas

Langkah pertama dalam menganalisis model adalah membentuk model PLS-SEM seperti yang ditunjukkan pada Gambar 2.



.

Gambar 2. Model Penelitian PLS

Tahap selanjutnya dalam menganalisis model adalah menganalisis uji validitas model PLS-SEM seperti pada Gambar 3.

.

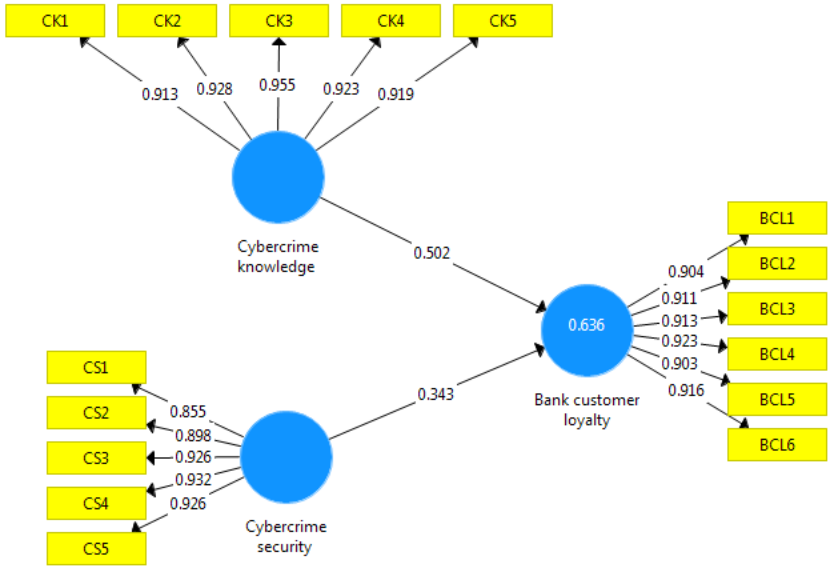


Fig 3 . ValidityTesting

Gambar 2 menunjukkan bahwa nilai semua outer loading berada di atas 0,5. Berdasarkan data yang disajikan pada Gambar 2, dapat disimpulkan bahwa semua indikator yang digunakan dalam penelitian ini telah memenuhi persyaratan dan dapat dikatakan valid.

4.3. Uji Reliabilitas

Tabel 1 merupakan hasil uji AVE yang menunjukkan bahwa variabel-variabel tersebut memiliki nilai AVE lebih besar dari 0,60 sehingga konstruk dapat disimpulkan reliabel.

.Table 1. AVE Testing

Variables	AVE Value
Cybercrime knowledge	0.645
Cybercrime security	0.612
Bank customer loyalty	0.687

Tabel 2 menunjukkan bahwa alpha Cronbach pada sebagian besar konstruk lebih dari 0,6, sehingga konstruk tersebut dapat disimpulkan reliabel.

.
Table 2. Cronbach's alpha Testing

Variables	Cronbach's alpha Value

Cybercrime knowledge	0.743
Cybercrime security	0.775
Bank customer loyalty	0.717

Tabel 3 menunjukkan bahwa nilai reliabilitas komposit pada seluruh konstruk lebih dari 0,7 sehingga dapat disimpulkan bahwa konstruk dalam penelitian ini reliabel.
Table 3. Cronbach's alpha Testing

Variables	composite reliability Value
Cybercrime knowledge	0.798
Cybercrime security	0.717
Bank customer loyalty	0.743

Tabel 4 menunjukkan bahwa nilai R2 dalam penelitian ini yang dapat dikatakan bahwa koefisien determinasi (R2) dalam penelitian ini mempunyai pengaruh yang kuat.

Table 3. Cronbach's alpha Testing

Variables	R2 value
Bank customer loyalty	0.636

Tabel 4 menunjukkan nilai Q2 lebih besar dari 0, yaitu 0,113, 0,176, dan 0,117, yang dapat diartikan bahwa hubungan antar variabel penelitian dianggap relevan. Berdasarkan perhitungan GoF di atas, nilai GoF dalam penelitian ini adalah 0,432, sehingga dapat dikatakan bahwa model yang digunakan memiliki tingkat kesesuaian yang relatif besar.
Table 4. Q2 Testing

Variables	Q2 Value
Cybercrime knowledge	0.113
Cybercrime security	0.176
Bank customer loyalty	0.117

4.4. Pengujian Hipotesis
Pengujian hipotesis digunakan untuk menentukan hubungan antar variabel dengan melihat hasil bootstrapping dari bagian t-statistik dan nilai-p. Syarat suatu hipotesis dalam penelitian tidak ditolak adalah jika nilai t-statistik lebih besar dari 1,96 dan nilai-p kurang dari 0,5. Gambar 3 dan Tabel 5 menunjukkan hasil bootstrapping yang telah dilakukan.

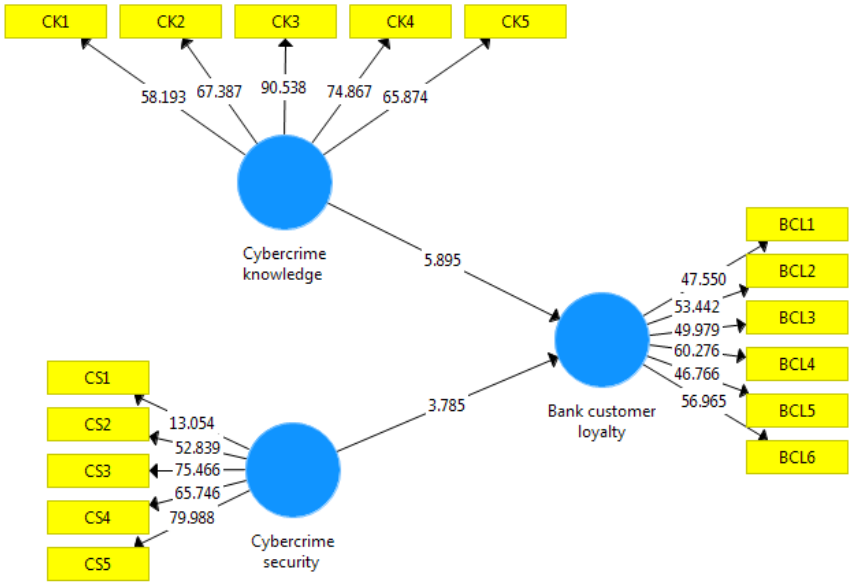


Figure 4. Hypothesis testing

Table 5. Hypothesis Testing

Correlation	P Value	T Values	Remark
Pengetahuan kejahatan siber - loyalitas nasabah bank	0.000 < 0.050	5.895 > 1.96	Supported
Keamanan kejahatan siber - loyalitas nasabah bank	0.000 < 0.050	3.785 > 1.96	Supported

4.5. Hubungan antara Pengetahuan Cybercrime dengan Loyalitas Nasabah Bank

Penelitian pada nasabah internet banking menghasilkan nilai koefisien jalur sebesar 0,502 (>0) pada variabel eksogen pengetahuan. Nilai T Statistik pada korelasi antara variabel eksogen pengetahuan dengan variabel endogen loyalitas nasabah menghasilkan nilai sebesar 4,895 (>1,96) dan nilai P-nya sebesar 0,000 (<0,05) hasil data tersebut menunjukkan bahwa pengetahuan cybercrime memiliki hubungan positif signifikan terhadap loyalitas nasabah bank. Maka hipotesis dalam penelitian ini adalah pengetahuan berpengaruh positif signifikan terhadap loyalitas nasabah bank[33]. Oleh karena itu, hipotesis dalam penelitian ini dapat diterima. Pengetahuan sumber daya manusia terhadap permasalahan cybercrime diharapkan dapat ditingkatkan lagi untuk dapat mengatasi permasalahan yang berkaitan dengan cybercrime, dengan harapan masyarakat baik mahasiswa maupun masyarakat secara keseluruhan dapat turut berpartisipasi dalam upaya penanggulangan cybercrime. Tidak hanya itu saja, masyarakat

khususnya mahasiswa harus memahami dan mengetahui dasar hukum serta landasan yang mengatur tentang kejahatan dunia maya atau yang kita kenal dengan istilah cybercrime[34]. Dari hasil penelitian ini sejalan dengan penelitian bahwa hasil pengetahuan tentang cybercrime memberikan kemudahan bagi kehidupan manusia, namun kemajuan tersebut juga dapat menimbulkan berbagai permasalahan yang tidak mudah untuk dicarikan jalan keluarnya. Salah satu permasalahan yang akan timbul seiring dengan kemajuan teknologi informasi adalah lahirnya kejahatan dalam bentuk-bentuk baru terutama yang memanfaatkan internet sebagai sarana kejahatannya atau yang dikenal dengan istilah cybercrime. Hasil penelitian ini menunjukkan bahwa pengetahuan nasabah tentang cybercrime berpengaruh positif signifikan dan diterima. Pengetahuan berkaitan dengan hal-hal yang positif yaitu dapat mencegah terjadinya risiko-risiko yang dapat merugikan nasabah. Kemudahan pelayanan yang diberikan oleh bank berkaitan dengan layanan e-banking salah satunya dimana e-banking dinilai memiliki kelebihan dimana dengan e-banking nasabah dapat memenuhi transaksi sehari-hari, pemenuhan transaksi secara cepat, mudah, efektif dan efisien menjadi salah satu faktor tercapainya kepuasan nasabah. Apabila faktor kepuasan terpenuhi maka kepuasan nasabah akan meningkat dan apabila faktor dalam pencapaian kepuasan nasabah kurang maka tingkat kepuasan nasabah akan menurun, dan menurunnya kepuasan akan mengakibatkan kerugian bagi bank yaitu akan kehilangan loyalitas nasabah[35].

4.6. Hubungan antara Keamanan Kejahatan Siber dengan Loyalitas Nasabah Bank

Penelitian pada pengguna internet banking menghasilkan nilai koefisien jalur sebesar 0,343 (<0) pada variabel keamanan eksogen. Nilai T Statistik pada korelasi antara variabel keamanan eksogen dengan variabel loyalitas nasabah endogen menghasilkan nilai sebesar 3,785 (>1,96) dan nilai P-nya sebesar 0,000 (<0,05) hasil data tersebut menunjukkan bahwa keamanan kejahatan siber memiliki hubungan positif signifikan terhadap loyalitas nasabah bank. Maka hipotesis dalam penelitian ini adalah keamanan berpengaruh positif signifikan terhadap loyalitas nasabah bank syariah. Oleh karena itu, hipotesis dalam penelitian ini dapat diterima. Keamanan dalam kejahatan siber merupakan tindakan untuk melindungi informasi di dunia maya dari berbagai serangan[36]. Kejahatan siber semakin marak terjadi karena semakin meningkatnya penggunaan komputer seperti desktop, komputer, laptop, smartphone, server, dan perangkat lainnya. Hasil penelitian ini sejalan dengan penelitian bahwa hasil keamanan kejahatan siber menjadi topik utama penelitian. Di era teknologi dan informasi yang berkembang pesat, hal tersebut berdampak pada semua aspek kehidupan. Salah satunya adalah keamanan siber yang memiliki peran penting dalam mencegah kejahatan siber. Oleh karena itu, keamanan kejahatan siber memengaruhi loyalitas nasabah. Hasil penelitian ini juga menunjukkan bahwa keamanan dapat memengaruhi kepercayaan nasabah dalam menggunakan Internet banking. Jika nasabah mendapatkan kepercayaan, hal itu dapat membuat nasabah tetap loyal dalam menggunakan produk dan layanan di bank syariah. Pencegahan kejahatan siber dapat dilakukan melalui pencegahan dan penegakan hukum. Jika dibiarkan, hal itu dapat mengganggu keamanan baik

Vol. 6 No. 4 (2025): August 2025 https://www.ijosmas.org e-ISSN: 2775-0809

secara nasional maupun internasional. Kejahatan siber dilakukan dengan lebih menekankan pada serangan internet, oleh karena itu diperlukan adanya pengalaman sistem untuk mencegah baik secara nasional maupun internasional[37]. Faktor keamanan dalam penelitian ini memiliki pengaruh positif dan signifikan terhadap loyalitas nasabah. Objek penelitian ini memutuskan untuk tetap menggunakan layanan bank setelah tragedi kejahatan yang menyerang bank syariah Indonesia. Kemudahan dan kenyamanan yang ditawarkan oleh fasilitas layanan e-banking menjadi beberapa faktor yang diterima dengan baik dan diminati oleh nasabah. Kemudahan transaksi sehari-hari melalui layanan yang disediakan oleh e-banking yang diakses dalam layanan digital membuat nasabah merasa nyaman dalam bertransaksi. Kenyamanan merupakan suatu hal yang penting dalam memenuhi kepuasan nasabah selain kemudahan dan kenyamanan yang diberikan yang dapat meningkatkan minat nasabah dalam menggunakan layanan e-banking, keduanya dapat mempengaruhi kepuasan, dimana apabila layanan e-banking dapat diakses dengan mudah dan dapat meningkatkan kenyamanan maka tingkat kepuasan nasabah meningkat dengan baik. Layanan digital yang diberikan oleh bank memiliki keunggulan pada kecepatan akses dan kenyamanan dimana terdapat fitur keamanan yang menjaga keamanan data nasabah. Kejahatan dunia maya mempengaruhi kepuasan nasabah, dengan demikian bank harus memberikan pelayanan yang optimal kepada nasabah dengan memperkuat sistem keamanan. Meningkatnya kejahatan dunia maya dan e-banking keduanya memberikan dampak terhadap kepuasan. Keduanya berkaitan dengan kemajuan teknologi informasi dan komunikasi saat ini, hanya saja e-banking merupakan bentuk positif dari kemajuan teknologi sedangkan kejahatan dunia maya merupakan dampak negatif yang ditimbulkan oleh kemajuan teknologi yang ada[38].

Niat sebagai salah satu faktor yang mempengaruhi perilaku, telah ditetapkan dalam acuan sistem informasi dan disiplin ilmu lainnya. Sehingga mengarah pada adanya niat atau keinginan individu untuk melakukan kejahatan dunia maya atau berperilaku tidak etis saat menggunakan internet banking. Kejahatan dunia maya merupakan segala bentuk kegiatan yang berkaitan dengan kegiatan seseorang, kelompok, atau badan hukum dimana kegiatan tersebut menggunakan komputer sebagai sarana untuk melakukan kejahatan. Kejahatan dunia maya ini dapat berupa berbagai pengguna jaringan komputer yang bertujuan untuk melakukan kejahatan dengan teknologi tinggi dengan menyalahgunakan kemudahan teknologi digital yang ada. Oleh karena itu, kejahatan di dunia maya dapat muncul karena adanya kemungkinan terjadinya interaksi antara satu perangkat dengan perangkat lainnya yang saling terhubung. Dari hasil penelitian yang dikaji oleh penulis, penelitian ini sejalan dengan penelitian bahwa pengetahuan berpengaruh positif dan signifikan terhadap loyalitas pengguna e-banking bank syariah. Hal ini dapat diartikan bahwa nasabah yang memiliki pengetahuan umum tentang internet dapat merasa lebih yakin dengan pengetahuan yang dimilikinya, oleh karena itu dapat memperoleh loyalitas sebagai nasabah pengguna e-banking bank Hasil penelitian ini dapat menunjukkan bahwa hipotesis pengalaman nasabah berpengaruh positif dan signifikan terhadap penggunaan fasilitas e-banking karena banyaknya kasus kejahatan dunia maya disamping kemudahan dan manfaat

Vol. 6 No. 4 (2025): August 2025 https://www.ijosmas.org e-ISSN: 2775-0809

nasabah memiliki kekhawatiran terkait keamanan dalam bertransaksi[39]. Rasa aman dan percaya menjadi salah satu faktor yang mempengaruhi nilai kepuasan nasabah. Apabila nasabah memiliki tingkat kepercayaan yang tinggi maka kualitas dan tingkat kepuasan nasabah meningkat dan apabila kepercayaan memiliki presentase yang rendah maka tingkat kepuasan nasabah menurun. Dengan demikian dapat disimpulkan bahwa pernyataan kuesioner mempengaruhi variabel kepuasan. Dengan adanya keluhan akibat rasa khawatir dan takut maka pihak bank diharapkan dapat memaksimalkan sistem keamanan yang ada untuk melindungi data nasabah. Keamanan menjadi salah satu faktor dalam kepuasan nasabah yaitu pada bagian jaminan, apabila keamanan yang terdapat pada layanan e-banking ditingkatkan maka kepuasan nasabah akan meningkat apabila terjadi serangan kejahatan dunia maya, dan sistem keamanan yang diberikan oleh pihak bank dapat melindungi data nasabah. Kejahatan dunia maya merupakan kejahatan yang dapat menyerang kapan saja, baik berupa phishing maupun skimming[40]. Kerugian yang diakibatkan oleh serangan kejahatan dunia maya, baik finansial maupun non finansial, membuat nasabah khawatir dan takut untuk melakukan transaksi. Berdasarkan kasus-kasus yang pernah terjadi terkait kejahatan dunia maya, nasabah merasa khawatir atau takut menjadi korban kejahatan dunia maya. Hal ini sejalan dengan penelitian yang menyatakan bahwa terjadinya kejahatan dunia maya yang merugikan nasabah berdampak pada tingkat loyalitas dan kepuasan nasabah.

Kejahatan dunia maya sebagai kejahatan murni, dimana orang yang melakukan kejahatan tersebut dilakukan dengan sengaja, dimana orang tersebut dengan sengaja dan berencana untuk melakukan pengrusakan, pencurian, tindakan anarkis terhadap suatu sistem informasi atau sistem komputer[41]. Kejahatan dunia maya sebagai suatu perbuatan dimana kejahatan ini tidak jelas antara kriminal atau tidak karena ia membobol tetapi tidak merusak, mencuri atau melakukan tindakan anarkis terhadap sistem informasi atau sistem komputer. Hal ini biasa dilakukan oleh para hacker, dimana seorang hacker biasanya masuk ke dalam suatu sistem jaringan atau sistem komputer untuk mengetahui apakah sistem tersebut aman atau tidak, tidak ada yang dirusak oleh hacker, mereka murni menguji sistem tersebut yang nantinya dapat melakukan perbaikan terhadap sistem yang diretas. Pengawasan terhadap layanan internet oleh bank akan mencakup kepatuhan bank terhadap regulasi dan risiko terhadap produk internet banking. Pengecekan terhadap tingkat kepatuhan terhadap standar operasional yang telah disepakati antara bank dengan otoritas pengawas akan dilakukan secara rutin termasuk keamanan dalam penggunaan sistem informasi dan manajemen risikonya, baik dengan mengirimkan kuesioner maupun melakukan inspeksi. Fokus pengawasan juga akan mencakup aspek-aspek yang terkait dengan risiko operasional dan hukum bagi bank, terutama terkait dengan fraud, verifikasi informasi, dan kontinuitas sistem informasi. Untuk itu perlu diberikan sosialisasi kepada para pengawas dan pemeriksa terkait internet banking dan aspek-aspek pentingnya termasuk sistem keamanan, aspek hukum, dan risiko internet banking.

Perlindungan nasabah sangat penting untuk menciptakan kepercayaan dan kenyamanan nasabah dalam melakukan transaksi melalui internet banking. Karena risiko teknologi dalam internet banking sangat tinggi, ada kemungkinan nasabah akan mengalami kerugian karena datanya dicegat oleh hacker/cracker atau situs web yang memiliki nama domain yang hampir sama. Untuk itu, ada beberapa hal penting yang perlu diterapkan oleh bank untuk melindungi nasabahnya, antara lain adalah Piagam Klien: yang berisi pernyataan dan komitmen dari bank untuk menjalankan operasional internet banking yang aman, menjaga privasi informasi nasabah, memberikan layanan yang andal dan berkualitas, transparansi produk dan layanan, serta tanggapan yang cepat terhadap pertanyaan dan keluhan nasabah[14]. Kerahasiaan Data Nasabah (Kebijakan Privasi): Kerahasiaan informasi pribadi nasabah merupakan unsur penting kepercayaan dan keyakinan masyarakat terhadap sistem perbankan Indonesia, untuk itu perbankan Indonesia diharapkan dapat merumuskan dan menerapkan kebijakan dan langkah nyata untuk menjaga dan menghormati privasi informasi pribadi nasabah serta mengungkapkan kebijakan tersebut secara terbuka kepada masyarakat. Uji Coba: Untuk meningkatkan pemahaman nasabah dalam menggunakan layanan internet banking, bank dapat menyediakan panduan penggunaan dan pelatihan (uji coba) bagi nasabah dalam menggunakan fitur dan fungsi yang dapat diperoleh nasabah di kantor bank maupun di situs web bank berupa tanya jawab, program demo, dan sebagainya. Layanan Dukungan Nasabah: Bank wajib menyediakan layanan nasabah 24 jam (Customer Support Service) yang dapat dihubungi melalui telepon, surat elektronik, atau media lainnya untuk menjawab pertanyaan nasabah dan membantu nasabah yang mengalami kesulitan dalam mengoperasikan internet banking. Selain itu, bank wajib memiliki dan menyediakan informasi mengenai prosedur penyampaian pengaduan nasabah, misalnya berupa kemampuan bank untuk melakukan audit trail guna memberikan bukti balik apabila terjadi sengketa antara bank dan nasabah terkait suatu transaksi. Sosialisasi: Bank perlu mengambil langkah proaktif dengan memberikan edukasi berkelanjutan dan menjelaskan kepada nasabah hak dan kewajibannya serta bagaimana menjaga kerahasiaan data nasabah dalam melakukan aktivitas/transaksi di internet. Setiap kali terjadi perubahan sistem, terutama yang terkait dengan keamanan, integritas data, dan autentikasi, nasabah perlu diberikan informasi yang memadai agar dapat menggunakan sistem. Sebelum menawarkan produk/layanan perbankan Internet kepada nasabah, bank harus membuat pedoman penggunaan perbankan Internet bagi nasabahnya.

4. 4.7. Implikasi Penelitian
5. Disarankan bagi bank untuk memberikan edukasi dan sosialisasi secara berkala mengenai layanan e-banking agar nasabah terhindar dari kejahatan siber. Selain itu, diharapkan pula adanya perlindungan khusus bagi nasabah. Dengan adanya informasi ini, diharapkan dapat memberikan masukan kepada bank untuk meningkatkan kualitas keamanan pada layanan e-banking. Bagi Masyarakat, Penelitian ini memberikan informasi bahwa nasabah harus memperhatikan risiko-risiko yang dapat timbul akibat kejahatan siber. Dengan mengetahui

risiko-risiko tersebut, diharapkan nasabah dapat lebih waspada dan bijak dalam menggunakan layanan e-banking. Dampak kejahatan siber terhadap kepercayaan masyarakat tidak terlalu terasa karena masyarakat tidak memiliki rasa khawatir terhadap kejahatan siber. Pada layanan e-banking, nasabah dapat dengan mudah melakukan transaksi tanpa harus pergi ke gerai. Tersedianya sistem keamanan pada e-banking menjadi bukti bahwa dampak yang dirasakan oleh pengguna layanan e-banking tidak terlalu signifikan. Solusi agar terhindar dari kejahatan siber saat menggunakan layanan e-banking adalah dengan mengganti PIN atau password secara berkala, jangan lupa untuk selalu log out setelah menggunakan aplikasi mobile banking, jangan menggunakan WiFi publik, dan pastikan alamat website Bank aman dan tidak mencurigakan.

6. Dampak terhadap e-commerce Penggunaan aplikasi e-commerce dipengaruhi oleh Kejahatan Siber. Timbulnya kerugian bagi pengguna, berkurangnya kepercayaan pengguna terhadap e-commerce, pemberian kunci keamanan tambahan yang merepotkan, dan membutuhkan perlindungan hukum yang tinggi bagi pengguna merupakan indikator dalam e-commerce akibat Kejahatan Siber. Banyaknya kerugian yang dialami pengguna e-commerce akibat Kejahatan Siber berdasarkan hasil penelitian sangat mempengaruhi penggunaan e-commerce oleh pengguna di kemudian hari. Kejahatan Siber sangat merugikan bagi pengguna seperti kehilangan banyak waktu, kehilangan keuangan, atau kehilangan data. Dampak terhadap Perbankan Hasil penelitian ini menunjukkan bahwa lembaga keuangan memiliki risiko kejahatan yang lebih tinggi dibandingkan lembaga lainnya. Meningkatnya jumlah nasabah yang menggunakan fasilitas Internet banking dapat memberikan peluang bagi pelaku kejahatan siber untuk melakukan kejahatan terhadap nasabah. Mengingat era saat ini adalah era digital, semakin banyak orang yang memanfaatkan keahliannya dalam menggunakan teknologi dan tidak sedikit pula dari mereka yang menyalahgunakan teknologi tersebut. Dampak Kejahatan Siber Kurangnya pengawasan terhadap penggunaan internet menciptakan kejahatan siber. Kejahatan ini menggunakan akses internet yang tidak hanya terjadi pada satu wilayah. Terbatasnya jumlah ahli dalam melakukan penyidikan menjadi faktor yang mempengaruhi keberhasilan kepolisian dalam memberantas kasus kejahatan siber, dengan jumlah anggota ahli yang sangat minim menjadi kendala dalam memberantas kasus kejahatan siber tidak dapat diselesaikan dalam waktu yang efisien sehingga hal ini dimanfaatkan oleh para pelaku dalam menjalankan aksinya dengan lebih leluasa.] Dampak kejahatan siber dapat bervariasi. Pertama-tama, korbannya dapat berupa pengguna (orang atau organisasi) atau sistem komputer. Kedua, masing-masing dapat terpengaruh dengan cara yang sangat berbeda, dari kerusakan yang tidak terdeteksi hingga kerugian finansial yang besar dan bahkan efek yang halus dan tidak berwujud pada individu (seperti menanamkan rasa takut terhadap dunia maya). Kekhawatiran tentang kejahatan siber yang meluas telah ditanggapi dengan strategi global. Konvensi ini dibentuk oleh negara-negara untuk membangun komitmen internasional dalam mewaspadai kejahatan dunia maya, mendorong perumusan peraturan hukum guna memberantas kejahatan dunia maya, membangun kerja sama

internasional guna memberantas kejahatan dunia maya, dan melaksanakan strategi tanpa alasan untuk menangani kejahatan dunia maya.

7. Kesimpulan

Setelah melakukan beberapa langkah penelitian dan pengolahan data yang diperlukan dalam penelitian ini, dapat ditarik beberapa kesimpulan, yaitu hasil uji hipotesis korelasi pertama menunjukkan bahwa pengetahuan tentang kejahatan siber berpengaruh signifikan terhadap loyalitas nasabah, dapat pula diartikan bahwa pengetahuan nasabah berpengaruh terhadap loyalitas nasabah. Hasil uji hipotesis korelasi kedua menunjukkan bahwa keamanan tentang kejahatan siber berpengaruh positif dan signifikan terhadap loyalitas nasabah, dapat pula diartikan bahwa keamanan nasabah berpengaruh terhadap loyalitas nasabah. Penelitian ini belum sempurna, tentunya terdapat kekurangan dan kelebihan, terutama keterbatasan penelitian ini, yaitu untuk melakukan penelitian untuk masa yang akan datang agar bermanfaat sebagai penelitian selanjutnya untuk melakukan penelitian yang lebih optimal. Peneliti masih memiliki kekurangan dalam pengumpulan responden dimana metode Google form kurang efektif. Berdasarkan hasil penelitian yang diperoleh dari data yang telah dikumpulkan dan diolah, penelitian ini dapat berjalan dengan baik, namun alangkah baiknya apabila peneliti memberikan beberapa saran yang dapat bermanfaat dan juga berguna untuk penelitian selanjutnya. Penelitian ini diharapkan dapat menjadi pertimbangan bagi pihak perbankan untuk memberikan pengalaman yang lebih baik bagi nasabah. Diharapkan penelitian ini dapat menjadi acuan bagi pihak perbankan untuk meningkatkan kualitas pelayanan dan jaminan keamanan agar loyalitas nasabah senantiasa terjaga dan meningkatkan kepercayaan nasabah terhadap bank syariah. Diharapkan pihak perbankan dapat memberikan edukasi terkait cybercrime. Pada penelitian selanjutnya diharapkan dapat menyediakan sampel yang lebih banyak dalam pengolahan data.

Setelah adanya hasil penelitian ini, baik hasil analisis maupun simpulan di atas, maka penulis dapat memberikan beberapa saran bagi beberapa pihak yaitu, Penelitian ini memberikan informasi bahwa nasabah harus memperhatikan risiko yang dapat timbul dari serangan Cybercrime dengan mengetahui risiko yang dapat terjadi sewaktu-waktu kepada nasabah, oleh karena itu diharapkan nasabah Bank dapat waspada dan berhati-hati dalam setiap proses transaksi. Bagi peneliti selanjutnya, Diharapkan peneliti selanjutnya dapat menambahkan variabel lain yang dapat meningkatkan loyalitas nasabah atau kepercayaan nasabah seperti menambahkan variabel risiko reputasi pada perbankan. Penelitian ini memberikan informasi bahwa nasabah masih merasa khawatir ketika menggunakan Bank H karena takut akan diserang Cybercrime. Dengan informasi ini, diharapkan dapat memberikan masukan kepada bank untuk lebih meningkatkan keamanan layanan guna menghindari serangan kejahatan siber dan lebih intensif dalam mensosialisasikan keamanan dalam penggunaan layanan Bank. b. Diharapkan juga akan ada bentuk perlindungan bagi nasabah yang diatur secara khusus untuk melindungi nasabah dari kejahatan siber yang marak belakangan ini. Bank dapat membuat semacam aplikasi

unit untuk melaporkan setiap kejahatan siber dan membangun sistem pencegahan atau pertahanan anti-malware di seluruh server bank.

References

1. Setiawan, N., Tarigan, V. C. E., Sari, P. B., Rossanty, Y., Nasution, M. D. T. P., & Siregar, I. (2018). Impact of cybercrime in e-business and trust. Int. J. Civ. Eng. Technol, 9(7), 652-656.
2. Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. Computers & Security, 45, 58-74.
3. Ilchenko, O., Chumak, V., Kuzmenko, S., Shelukhin, O., & Dobrovinskyi, A. (2019). Fishing as a cybercrime in the Internet banking system: economic and legal aspects. J. Legal Ethical & Regul. Isses, 22, 1.
4. Muhtasim, D. A., Tan, S. Y., Hassan, M. A., Pavel, M. I., & Susmit, S. (2022). Customer satisfaction with digital wallet services: an analysis of security factors. International Journal of Advanced Computer Science and Applications, 13(1), 195-206.
5. Helmiawan, M. A., & Nasution, A. I. (2022). The Effect of Internet Banking Use and Customer Protection Against Cyber Crime at Bank Rakyat Indonesia. Journal of Islamic Economics and Business, 2(2), 170-183.
6. JosephNg, P. S., EricMok, Z. C., Phan, K. Y., Sun, J., & Wei, Z. (2025). Mitigating Social Media Cybercrime: Revolutionising with AES Encryption and Generative AI. Journal of Advanced Research in Applied Sciences and Engineering Technology, 46(2), 124-154.
7. Smith, A. D. (2004). Cybercriminal impacts on online business and consumer confidence. Online Information Review, 28(3), 224-234.
8. Amin, M. (2016). Internet banking service quality and its implication on e-customer satisfaction and e-customer loyalty. International journal of bank marketing, 34(3), 280-306.
9. Abbas, T., & Arif, K. (2023). End-users' Perception of Cybercrimes towards E-banking Adoption and Retention. Journal of Independent Studies and Research Computing, 21(1).
10. Helmiawan, M. A., & Nasution, A. I. (2022). The Effect of Internet Banking Use and Customer Protection Against Cyber Crime at Bank Rakyat Indonesia. Journal of Islamic Economics and Business, 2(2), 170-183.
11. Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security, 45, 58-74.
12. Lestari, S., Adawiyah, W. R., Alhamidi, A. L., Prayogi, J., & Haryanto, R. (2024). Navigating perilous seas: unmasking online banking frauds, perceived usefulness, fear of cybercrime and distrust in online banking. Safer Communities, 23(4), 444-464.

13. Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows?. Technological Forecasting and Social Change, 80(3), 541-555.
14. Nasution, M. D. T. P., Rossanty, Y., Siahaan, A. P. U., & Aryza, S. (2018). The phenomenon of cyber-crime and fraud victimization in online shop. Int. J. Civ. Eng. Technol, 9(6), 1583-1592.
15. Aneke, S. O., Nweke, E. O., Udanor, C. N., Ogbodo, I. A., Ezugwu, A. O., Uguwishiwu, C. H., & Ezema, M. E. (2020). Towards determining cybercrime technology evolution in Nigeria. Int J Lates Technol Eng Manage Appl Sci, 9, 37-43.
16. Wada, F., & Odulaja, G. O. (2012). Electronic banking and cyber crime in Nigeria-a theoretical policy perspective on causation. African Journal of Computing and ICT, 4(2), 69-82.
17. Shafiya, S., Amin, S., & Ali, M. H. (2023). Examining E-Satisfaction as Mediator between Banking Mobile Application Quality Factors and Consumers E-Loyalty. Academic Journal of Social Sciences (AJSS), 7(1), 001-016.
18. Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. Journal of Financial Crime, 27(3), 945-958.
19. Vitvitskiy, S. S., Kurakin, O. N., Pokataev, P. S., Skriabin, O. M., & Sanakoiev, D. B. (2021). Peculiarities of cybercrime investigation in the banking sector of Ukraine: review and analysis. Banks and Bank Systems, 16(1), 69-80.
20. Malik, M. S., & Islam, U. (2019). Cybercrime: an emerging threat to the banking sector of Pakistan. Journal of Financial Crime, 26(1), 50-60.
21. Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. International Journal of Current Research & Academic Review, 2(2), 173-178.
22. Aribake, F. O. (2015). Impact of ICT tools for combating cyber crime in Nigeria online banking: a conceptual review. International Journal of Trade, Economics and Finance, 6(5), 272.
23. Ibrahim, U. M. A. R. U. (2019). The Impact of Cybercrime on the Nigerian Economy and banking system. NDIC Quarterly, 34(12), 1-20.
24. Ilchenko, O., Chumak, V., Kuzmenko, S., Shelukhin, O., & Dobrovinskyi, A. (2019). Fishing as a cybercrime in the Internet banking system: economic and legal aspects. J. Legal Ethical & Regul. Isses, 22, 1.
25. Wada, F., & Odulaja, G. O. (2012). Electronic banking and cyber crime in Nigeria-a theoretical policy perspective on causation. African Journal of Computing and ICT, 4(2), 69-82.
26. Ogunwale, H. (2020). The impact of cybercrime on Nigeria's commercial banking system. International Journal of Management and Business Studies, 2(3), 75-78.

27. Rao, H. S. (2019). Cyber crime in banking sector. International Journal of Research-Granthaalayah, 7(1), 148-161.
28. Goel, S. (2016). Cyber-Crime: A growing threat to Indian banking sector. International Journal of Science Technology and Management, 5(12), 552-559.
29. Suja, P., & Raghavan, N. (2014). Cybercrime in banking sector. International Journal of Research in Social Sciences, 4(1), 189-194.
30. Orji, U. J. (2019). Protecting consumers from cybercrime in the banking and financial sector: an analysis of the legal response in Nigeria. Tilburg Law Review, 24(1), 105-124.
31. Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. European Journal on Criminal Policy and Research, 23, 287-300.
32. Malik, S., Noreen, S., & Awan, A. G. (2018). The impact of cybercrimes on the efficiency of banking sector of Pakistan. Global Journal of Management, Social Sciences and Humanities, 4(4), 821-842.
33. Gaol, F. L., Budiansa, A. D., Weniko, Y. P., & Matsuo, T. O. K. U. R. O. (2021). Cyber crime risk control in non-banking organizations. Journal of Theoretical and Applied Information Technology, 99(5), 1219-1231.
34. Tabassum, L. (2020). State of Cyber Crime Safety and Security in Banking. Int. J. Sci. Res. Engineering Dev, 3(4), 72-76.
35. Lemieux, M. (2015). Cyber crime, governance and liabilities in the banking and payment industries. Banking & Finance Law Review, 31(1), 113-134
36. Spulbar, C., & Birau, R. (2020). The Effects of Cybercrime on the Banking Sector in ASEAN. In Financial Technology and Disruptive Innovation in ASEAN (pp. 130-148). IGI Global.
37. Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. International Journal of Law, Crime and Justice, 62, 100415.
38. Abdulazeez, H., Magaji, S., & Musa, I. (2022). Analysis of Infrastructural Challenges, Cybercrime, and the Cashless Policy in Nigeria: Infrastructural Challenges, Cybercrime, and the Cashless Policy. ARIS2-Advanced Research on Information Systems Security, 2(1), 13-27.
39. Singleton, T., Singleton, A., & Gottlieb, G. (2006). Cyberthreats Facing the Banking Industry. Bank Accounting & Finance (08943958), 19(2).
40. Akinbowale, O. E., Klingelhöfer, H. E., Zerihun, M. F., & Mashigo, P. (2024). Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. Heliyon, 10(1).12-19
41. Chitimira, H., & Ncube, P. (2021). The regulation and use of artificial intelligence and 5g technology to combat cybercrime and financial crime in south african banks.

Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad, 24(1).23-29