Bussman Journal: Indonesian Journal of Business and Managemen
p-ISSN: 2797-9725 | e-ISSN: 2777-0559
Vol. 5 No. 2 Mei - Agustus 2025

PENGARUH *RANSOMWARE* DAN *PHISHING* TERHADAP TINGKAT PEMAHAMAN MAHASISWA TENTANG KEJAHATAN SIBER

Gelora Chita Siahaan[1], Aminah[2]
[1,2]Universitas Bandar Lampung
Email: gelora.21021039@student.ubl.ac.id, aminah@ubl.ac.id

Abstract

This study aims to identify the level of understanding of FEB UBL students regarding ransomware and phishing threats, as well as to determine the extent of students' preparedness in facing such attacks. This study applies a quantitative method by utilizing primary data collected through questionnaires. The study population consists of 225 students from the Faculty of Economics and Business, Class of 2021, who have completed their final projects. The sample selection used the Slovin formula at 10%, resulting in 70 respondents. The analysis concluded that ransomware and phishing significantly influence students' understanding of cybercrime.
***Keywords**: Ransomware, Phishing, Cybercrime, Student Understanding Level*

Abstrak

Penelitian ini bertujuan untuk mengidentifikasi tingkat pemahaman mahasiswa FEB UBL terhadap ancaman *ransomware* dan *phishing*, serta mengetahui sejauh mana kesiapan mahasiswa dalam menghadapi serangan tersebut. Penelitian ini menerapkan metode kuantitatif dengan memanfaatkan data primer yang dikumpulkan melalui kuesioner. Populasi penelitian ini yaitu mahasiswa Fakultas Ekonomi dan Bisnis Angkatan 2021 yang telah menyusun tugas akhir dengan jumlah 225. Pemilihan sampel menggunakan rumus *slovin* 10% menghasilkan 70 sampel sebagai responden. Dari hasil analisis maka disimpulkan *ransomware* dan *phishing* berpengaruh terhadap tingkat pemahaman mahasiswa tentang kejahatan siber
Kata kunci: *Ransomware, Phishing,* Kejahatan Siber, Tingkat Pemahaman Mahasiswa

PENDAHULUAN

Undang-Undang Nomor 11 Tahun 2008 di revisi dengan Undang-Undang Nomor 19 Tahun 2016 tentang informasi dan transaksi elektronik, bentuk-bentuk kejahatan siber (cyber crime) adalah tindak pidana yang berhubungan dengan aktivitas illegal, tindak pidana yang berhubungan dengan gangguan (interferens), tindak pidana memfasilitasi perbuatan yang dilarang, dan tindak pidana pemalsuan informasi atau dokumen elektronik berbasis teknologi (Rompi & Muaja, 2021). Perkembangan teknologi terus berlangsung seiring dengan meningkatnya kebutuhan manusia, mendorong lahirnya berbagai inovasi baru. Bukti nyata dari perkembangan ini dapat dilihat dari banyaknya penemuan berbasis teknologi, seperti gadget, laptop, televisi, pendingin udara, komputer pribadi (PC), gelombang radio, dan lain sebagainya (Hartono, 2023)

Kemajuan dan perkembangan teknologi tidak hanya memberikan pengaruh positif bagi masyarakat, tetapi juga memunculkan efek negatif yang tak dapat dihindari dalam

penggunaannya. Salah satu contoh nyata dari dampak negatif tersebut adalah kejahatan siber. Kejahatan siber, atau yang dikenal sebagai cybercrime, merupakan pelanggaran yang hanya bisa terjadi melalui penggunaan komputer, jaringan komputer, atau berbagai jenis teknologi komunikasi dan informasi (Kwarto & Angsito, 2018). Generasi digital memiliki keterkaitan erat dengan teknologi, baik dalam kegiatan akademik maupun kehidupan sehari-hari. Namun, keterpaparan mahasiswa terhadap ancaman siber, terutama ransomware dan phishing, masih cukup tinggi. Hal ini diperparah oleh kurangnya edukasi mengenai praktik keamanan digital, seperti cara mengenali serangan phishing dan menghindari tautan berbahaya yang disematkan dalam email atau situs palsu.

Pembelajaran akademik di perguruan tinggi sudah menggunakan perangkat teknologi untuk mengakses sistem pembelajaran daring, mengirim tugas, serta bertransaksi secara digital. Aktivitas ini meningkatkan risiko mahasiswa menjadi target empuk kejahatan siber, terutama phishing yang menyamar sebagai pesan akademik resmi dan ransomware yang dapat menyandera data penting (Faizal et al., 2023). Meskipun ransomware dan phishing adalah serangan siber yang berbeda, keduanya sering digunakan oleh peretas untuk mengeksploitasi kelemahan sistem keamanan dan sering digunakan bersamaan dalam serangan yang lebih besar.

Ransomware merupakan jenis perangkat lunak berbahaya, atau yang dikenal sebagai malware, yang dirancang untuk mengenkripsi data atau sistem komputer milik korban. Setelah itu, pelaku akan meminta sejumlah pembayaran sebagai syarat agar data atau sistem tersebut dapat diakses kembali. Ransomware biasanya menyebar melalui email phishing, situs web berbahaya, atau perangkat lunak yang terinfeksi. Serangan ransomware dapat menargetkan orang, perusahaan, bahkan infrastruktur vital, dan dapat menyebabkan kerugian besar uang dan reputasi (Shiring et al., 2024). Ransomware bekerja dengan cara mengenkripsi data pengguna dan menuntut tebusan dalam mata uang kripto sebagai syarat memulihkannya. Ransomware menyebar melalui email yang mengandung lampiran berbahaya dengan memanfaatkan celah keamanan dalam perangkat lunak. Setelah data berhasil dienkripsi, korban diharuskan membayar tebusan agar mendapatkan kunci dekripsi. Serangan ini sering menyasar individu maupun organisasi, termasuk institusi pendidikan.

Bagi mahasiswa, kehilangan akses ke data penting seperti tugas, catatan kuliah, atau dokumen pribadi dapat menghambat proses belajar (Dianita et al., 2022)

Phishing adalah teknik penipuan yang digunakan oleh peretas untuk mendapatkan data pribadi seperti username, password, nomor kartu kredit, atau lainnya. Mereka melakukan ini dengan menyamar sebagai orang yang dapat dipercaya (Hidayat et al., 2023) Serangan phishing biasanya dilakukan melalui email yang terlihat seperti berasal dari sumber resmi, seperti bank, layanan online, atau perusahaan terkenal. Email yang dikirim mengandung tautan atau lampiran berbahaya yang dapat membawa korban ke situs web palsu yang meniru halaman login resmi. Phishing biasanya digunakan untuk mendapatkan akses awal yang memungkinkan serangan ransomware, dengan peretas mengirimkan malware melalui email sehingga peretas dapat mengambil informasi pribadi korban untuk melakukan pencurian identitas, penipuan finansial, atau bahkan mengakses sistem yang lebih besar untuk serangan lainnya (Saputra Gulo et al., 2020) Serangan phishing dilakukan melalui panggilan telepon palsu atau pesan teks yang dirancang untuk menipu mahasiswa agar mengungkapkan informasi pribadi mereka. Mahasiswa yang kurang waspada terhadap ancaman siber, menjadi salah satu target utama serangan phishing (Fatimah et al., 2020).

Hubungan antara Ransomware dan Phishing: Phishing biasanya menjadi dasar serangan ransomware. Peretas seringkali menggunakan email phishing untuk menyebarkan malware ransomware. Setelah korban membuka lampiran atau mengklik tautan yang terinfeksi, ransomware dapat masuk ke perangkat mereka dan mengenkripsi data mereka dan meminta pembayaran. Oleh karena itu, serangan phishing dan ransomware sering berjalan bersamaan, dan phishing berfungsi sebagai pintu masuk untuk penyebaran ransomware (Surya Kusuma, 2023)

Sistem administrasi kampus yang sepenuhnya berbasis online rentan terhadap serangan phishing atau penipuan untuk memperoleh data dan informasi. Di dunia maya, pelaku kejahatan dapat menemukan cara untuk meretas sistem ini dengan menargetkan siswa, staf, dan dosen yang memiliki celah keamanan. Olga Svistunova, pakar keamanan siber dari Kaspersky, mengungkapkan adanya kampanye phishing yang intens, di mana penipu memanfaatkan nama-nama universitas terkemuka di dunia. Biasanya, phishing dilakukan dengan membuat situs palsu yang meniru halaman resmi universitas dengan

sangat mirip (https://www.detik.com/). Kurangnya pemahaman mahasiswa tentang keamanan siber menjadi salah satu faktor utama yang membuat mereka rentan terhadap serangan ransomware dan phishing. Minimnya kesadaran untuk mengenali ciri-ciri serangan ransomware dan phishing dapat meningkatkan risiko kerugian, baik secara akademik maupun finansial (Fatkhur Rohmah, 2023).Penting untuk mengidentifikasi bagaimana ransomware dan phishing memengaruhi mahasiswa serta mencari solusi untuk meningkatkan kesadaran dan kesiapan mereka dalam menghadapi ancaman siber (Tan et al., 2024)

Novelty dalam penelitian ini adalah penggabungan dua ancaman siber utama yaitu ransomware dan phishing untuk melihat dampaknya terhadap tingkat pemahaman mahasiswa. Fokus pada mahasiswa sebagai subjek penelitian memberikan perspektif baru, sebagian besar penelitian sebelumnya berpusat pada organisasi atau masyarakat umum. Penelitian ini mengisi kesenjangan literatur dengan menjadikan tingkat pemahaman mahasiswa sebagai variabel dependen yang jarang dibahas dalam konteks kejahatan siber.

Pentingnya penelitian ini, mahasiswa dapat memahami potensi resiko yang ada dalam dunia digital dan dapat mendukung terciptanya lingkungan digital yang aman di kalangan generasi muda. Penelitian ini juga relevan untuk mendukung upaya institusi pendidikan dalam melindungi generasi muda dari ancaman dunia digital dan dapat meningkatkan literasi keamanan siber. Penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan kesadaran keamanan siber di kalangan mahasiswa dan merumuskan upaya pencegahan yang efektif di lingkungan kampus.

Tujuan penelitian ini untuk menguji pengaruh ransomware dan phising terhadap tingkat pemahaman mahasiswa dalam mengantisipasi ancaman siber. Penelitian ini juga memberikan wawasan yang dapat digunakan untuk menyusun strategi edukasi atau kebijakan guna meningkatkan kesadaran dan keamanan siber khususnya dilingkungan kampus (Fenny Anita & Tanujaya, 2023).

Manfaat penelitian ini bagi penulis dapat memberikan kesempatan untuk memperdalam pemahaman mengeni ancaman siber, ransomware dan phishing. Penulis dapat meningkatkan kemampuan analisis dan kontribusi akademis dalam bidang keamanan siber. Dengan hasil penelitian ini, kampus dapat merancang program edukasi dan pelatihan

keamanan siber untuk meningkatkan literasi digital mahasiswa. Penelitian ini juga dapat membantu kampus memitigasi risiko serangan siber di lingkungan akademik, menciptakan ekosistem digital yang lebih aman dan mendukung perkembangan teknologi

KAJIAN PUSTAKA DAN PENGEMBANGAN HIPOTESIS

Kejahatan Siber

Kejahatan siber adalah tindakan kejahatan yang dengan memanfaatkan teknologi komputer dan internet sebagai sarana utama dalam menjalankan aksinya. Cybercrime merupakan bentuk pelanggaran hukum yang timbul seiring dengan kemajuan teknologi computer (Rani Azura et al., 2021). Secara definisi, kejahatan siber merujuk pada perbuatan melanggar hukum yang menggunakan teknologi komputer dan didukung oleh perkembangan pesat teknologi internet. Kejahatan siber merupakan dimensi baru dari tindak kriminal yang mendapat perhatian besar di tingkat internasional. Istilah lain yang digunakan untuk menggambarkan jenis kejahatan ini meliputi kejahatan dunia maya (cyber space), kejahatan teknologi tinggi (high tech crime), kejahatan lintas negara (transnational crime), serta kejahatan kerah putih (white collar crime). Meskipun teknologi membawa banyak kemajuan, sisi gelapnya juga hadir dalam bentuk kejahatan siber yang berdampak luas pada berbagai aspek kehidupan (Arofah & Priatnasari, 2020). Kejahatan siber yang sering disebut sebagai cybercrime, merujuk pada tindakan kriminal yang dilakukan melalui komputer dan jaringan internet. Pelaku kejahatan siber umumnya akan meretas sistem untuk mengakses data pribadi korban. (Butarbutar, 2023).

Kejahatan dunia maya adalah aktivitas ilegal yang terjadi di dunia digital dengan tujuan menipu organisasi atau individu, bahkan merusak fungsi komputer. Tindakan kriminal ini melibatkan akses ilegal atau tidak sah, persimpangan ilegal yang melibatkan sarana teknis transmisi data komputer non-publik ke dan dari atau di dalam sistem komputer dan gangguan data yang mencakup kerusakan, penghapusan, penurunan kualitas, perubahan, penekanan data komputer yang tidak sah (Ugbomah et al., 2022)

Ransomware

Ransomware adalah jenis perangkat lunak berbahaya, atau perangkat lunak berbahaya yang mengintimidasi korban dengan merusak dan membatasi akses ke data atau

sistem vital sampai tebusan dibayar. Sebagian besar serangan ransomware dikendalikan oleh manusia yang menargetkan organisasi semakin meluas dan semakin sulit untuk dicegah maupun diatasi. Dalam serangan ransomware yang dilakukan manusia, kelompok penyerang memanfaatkan informasi yang telah mereka kumpulkan untuk mendapatkan akses ke jaringan perusahaan. Beberapa serangan semacam ini sangat canggih, hingga penyerang dapat menggunakan dokumen keuangan internal yang ditemukan untuk menentukan besaran tebusan yang diminta (Beaman et al., 2021).

Ada 2 bentuk utama ransomware yaitu :

1. *Ransomware* Kripto

   Ransomware kripto mengenkripsi jenis file tertentu yang dianggap berharga bagi korban seperti dokumen, *spreadsheet*, gambar, dan basis data. *Ransomware* ini dapat menggunakan enkripsi simetris, asimetris, atau hibrida. Pada individu atau organisasi yang menjadi target serangan, penyerang akan mengenkripsi data atau file sensitif sehingga korban tidak dapat mengaksesnya kecuali membayar tebusan yang diminta. Setelah pembayaran dilakukan, korban akan diberikan kunci enkripsi untuk mendapatkan kembali akses ke data atau file tersebut. Meskipun tebusan telah dibayar, tidak ada jaminan pelaku kejahatan siber akan memberikan kunci enkripsi data tersebut (Sainuri Mubarak *et al*., 2024).

2. *Ransomware Locker*

   Pada serangan *ransomware locker*, korban akan terkunci dari perangkat dan tidak dapat mengaksesnya. Layar perangkat akan menampilkan pesan tebusan yang memberitahukan bahwa akses mereka telah diblokir, beserta petunjuk untuk membayar tebusan untuk mendapatkan kembali akses. *Ransomware* ini biasanya tidak melibatkan enkripsi, setelah korban mendapatkan kembali akses ke perangkat mereka, file dan data sensitif tetap aman (Gómez-Hernández *et al*., 2021)

Phishing

Phishing merupakan usaha untuk memperoleh informasi pribadi seseorang dengan cara menipu. Data yang menjadi target phishing meliputi informasi pribadi (seperti nama, usia, alamat), data akun (username dan password), serta data finansial (seperti informasi kartu kredit atau rekening bank). Istilah phishing sendiri berasal dari kata "fishing" dalam

bahasa Inggris, yang berarti memancing. Tujuan dari phishing adalah untuk "memancing" korban agar secara sukarela memberikan informasi pribadi tanpa menyadari bahwa informasi tersebut akan digunakan untuk tujuan kriminal (Caniago & Sutabri, 2023).

Phishing adalah tindakan menipu pengguna komputer di internet (user) untuk memberikan informasi pribadi mereka, seperti username dan password, pada situs web yang telah dipalsukan. Serangan phishing sering kali ditargetkan pada pengguna layanan perbankan online. Data pribadi dan kata sandi yang dimasukkan oleh korban kemudian akan dimiliki oleh pelaku kejahatan dan digunakan untuk melakukan pembelian dengan kartu kredit atau menarik uang dari rekening korban (Setia Buana et al., 2023)

Phishing merupakan tindakan kriminal yang memanfaatkan teknik rekayasa sosial. Pelaku phishing, yang sering disebut sebagai phisher, berusaha memperoleh informasi pribadi seperti nama pengguna, kata sandi, dan rincian kartu kredit, yang kemudian dapat digunakan untuk pencurian identitas (Vadila & Pratama, 2021). Pengguna internet yang kurang waspada menjadi target utama para penjahat cyber dalam melancarkan aksi phishing (Syah, 2023). Ini disebabkan oleh beberapa faktor, salah satunya adalah minimnya edukasi dan literasi digital yang membuat banyak orang tidak memahami cara kerja phishing dan bagaimana cara melindungi diri dari kejahatan tersebut. Selain itu, ketidakhati-hatian pengguna yang sering tergoda dengan tawaran menarik atau informasi yang tampak kredibel tanpa verifikasi terlebih dahulu, serta teknologi phishing yang semakin canggih, turut meningkatkan risiko menjadi korban (Wijaya & Nurnawati, 2022)

Hubungan antara Ransomware dan Phishing :

Beberapa langkah penting yang dapat diambil untuk mencegah serangan ransomware dan phishing meliputi:

1. Pelatihan Pengguna untuk memberikan informasi kepada pengguna tentang risiko *phishing* dan cara membedakan email atau pesan yang mencurigakan.
2. Keamanan sistem dengan menggunakan perangkat keamanan seperti antivirus dan *firewall* untuk mendeteksi dan mencegah infeksi dan memperbarui perangkat lunak secara teratur.
3. Cadangan data dibuat secara teratur mencadangkan informasi penting sehingga dapat dipulihkan dalam kasus serangan *ransomware.*

4. Verifikasi keaslian setiap kali menerima komunikasi, terutama jika Anda meminta informasi pribadi atau pembayaran.
5. Individu dan organisasi dapat mengurangi risiko dan dampak dari ancaman siber dengan memperoleh pemahaman yang lebih baik tentang *ransomware* dan *phishing* serta langkah-langkah pencegahan yang tepat (Arifina *et al*., 2022).

Pengembangan Hipotesis

Ransomware

Ransomware adalah jenis malware yang mengenkripsi data pengguna dan meminta pembayaran tebusan agar data tersebut bisa dipulihkan. Malware ini bekerja dengan mengenkripsi data di sistem korban, kemudian menuntut pembayaran dalam bentuk mata uang kripto untuk mengembalikan akses ke data tersebut. Ransomware umumnya menyebar melalui email yang berisi lampiran berbahaya atau dengan mengeksploitasi celah keamanan dalam perangkat lunak. Setelah berhasil mengenkripsi data, korban diharuskan membayar tebusan untuk memperoleh kunci dekripsi (Larasati & Firdaus, 2024). Ransomware sering kali menargetkan individu dan organisasi, termasuk lembaga pendidikan. Bagi mahasiswa, kehilangan akses ke data penting seperti tugas, catatan kuliah, atau dokumen pribadi dapat menghambat proses belajar. Serangan ransomware ini memberikan dampak besar, memengaruhi lebih dari 200 instansi pemerintah dengan konsekuensi yang luas. Layanan publik seperti kesehatan, imigrasi, dan pendidikan mengalami gangguan serius, termasuk penundaan akses ke data pasien di rumah sakit yang mengakibatkan keterlambatan perawatan. Selain itu, proses pengurusan dokumen imigrasi terhambat, yang mengganggu perjalanan internasional (Rosa et al., 2024). Dari sisi ekonomi, serangan ini menimbulkan kerugian finansial yang diperkirakan mencapai miliaran rupiah, mencakup biaya pemulihan sistem, kehilangan pendapatan akibat terganggunya layanan, dan potensi denda akibat pelanggaran perlindungan data. Selain itu, data pribadi warga, termasuk informasi kesehatan dan keuangan, berisiko bocor. Pelaku serangan semakin menambah tekanan dengan ancaman untuk membocorkan data tersebut jika tebusan tidak dibayar, menciptakan tantangan besar bagi pemerintah dalam menangani situasi ini. (Simorangkir et al., 2024)

H_1 : *Ransomware* berpengaruh signifikan terhadap tingkat pemahaman mahasiswa *Phishing*

Berdasarkan analisis data, ditemukan bahwa phishing memiliki dampak positif dan signifikan terhadap penerimaan opini audit kepatuhan cybersecurity di sektor keuangan, sehingga hipotesis dapat diterima. Kejahatan ini paling sering terjadi di sektor keuangan, terutama yang melibatkan nasabah bank. Pelaku dapat melakukan berbagai transaksi yang seolah-olah dilakukan oleh nasabah yang identitasnya telah dicuri. Hal ini mendorong pemerintah, sebagai pihak yang bertanggung jawab atas semua sektor di Indonesia, untuk menetapkan kebijakan guna meningkatkan kesadaran tentang pentingnya keamanan siber, termasuk di sektor keuangan (Kwarto & Angsito, 2018)

H_2 : *Phishing* berpengaruh signifikan terhadap tingkat pemahaman mahasiswa

METODE PENELITIAN

Jenis dan Metode Penelitian

Penelitian ini menggunakan metode kuantitatif dengan pendekatan deskriptif-asosiatif untuk menganalisis pengaruh ransomware dan phishing terhadap tingkat pemahaman mahasiswa tentang kejahatan siber. Metode kuantitatif dipilih karena memungkinkan peneliti untuk mengukur dan menganalisis data secara numerik, yang bertujuan untuk menguji hipotesis yang telah dirumuskan (Sugiyono, 2023). Pendekatan ini memungkinkan peneliti untuk mengumpulkan data dari populasi yang luas dan membuat generalisasi dari hasil yang diperoleh (Sudaryono, 2021). Jenis penelitian deskriptif-asosiatif bertujuan untuk mendeskripsikan variabel-variabel yang diteliti dan melihat hubungan sebab-akibat atau pengaruh antara variabel independen (ransomware dan phishing) terhadap variabel dependen (tingkat pemahaman mahasiswa) (Emzir, 2024).

Populasi dan Sampel

Populasi dalam penelitian ini adalah mahasiswa Fakultas Ekonomi dan Bisnis (FEB) Universitas Bandar Lampung angkatan 2021 yang telah menyusun tugas akhir, dengan total 225 mahasiswa. Keterbatasan waktu dan biaya menjadi pertimbangan dalam menentukan populasi dan sampel (Arofah & Priatnasari, 2020). Pengambilan sampel dilakukan menggunakan rumus Slovin dengan tingkat toleransi 10%. Rumus tersebut menghasilkan

jumlah sampel sebanyak 69,23 yang kemudian dibulatkan menjadi 70 responden. Penggunaan rumus Slovin ini memastikan ukuran sampel yang representatif dari populasi, sehingga hasil penelitian dapat diandalkan (Fenny Anita & Tanujaya, 2023).

Instrumen dan Teknik Analisis Data

Data primer dikumpulkan melalui kuesioner yang disebarkan secara daring kepada 70 responden yang merupakan pengguna smartphone dan internet (Arofah & Priatnasari, 2020). Kuesioner ini disusun menggunakan skala Likert dan terdiri dari 30 pertanyaan yang mencakup variabel kejahatan siber, ransomware, dan phishing (Fenny Anita & Tanujaya, 2023). Setiap variabel diukur menggunakan 10 pertanyaan untuk memastikan cakupan yang komprehensif. Setelah data terkumpul, analisis data dilakukan menggunakan program SPSS versi 17. Teknik analisis data yang diterapkan meliputi uji validitas, uji reliabilitas, uji normalitas, uji multikolinearitas, regresi linear berganda, serta uji F dan uji t (Ghozali, 2012).

Prosedur Penelitian

Prosedur penelitian ini diawali dengan studi literatur untuk merumuskan landasan teori terkait ransomware dan phishing serta tingkat pemahaman mahasiswa (Faizal et al., 2023; Hidayat et al., 2023). Selanjutnya, kuesioner disusun dan divalidasi oleh pakar untuk memastikan pertanyaan yang relevan dan dapat mengukur variabel dengan tepat (Caniago & Sutabri, 2023). Kuesioner kemudian disebarkan secara daring kepada sampel yang telah ditentukan. Setelah data terkumpul, dilakukan proses pengolahan dan analisis data menggunakan perangkat lunak SPSS. Langkah pertama dalam analisis data adalah melakukan uji validitas dan reliabilitas untuk memastikan instrumen penelitian konsisten dan akurat (Rani Azura et al., 2021). Kemudian, dilakukan uji asumsi klasik, seperti uji normalitas dan multikolinearitas, untuk memenuhi persyaratan model regresi linear berganda (Butarbutar, 2023). Terakhir, dilakukan analisis regresi linear berganda serta uji F dan uji t untuk menguji hipotesis yang diajukan. Hasil dari uji ini digunakan untuk menarik kesimpulan mengenai pengaruh ransomware dan phishing terhadap tingkat pemahaman mahasiswa tentang kejahatan siber (Tan et al., 2024).

HASIL PENELITIAN

1. **Uji Validitas**

Tabel 1. Uji Validitas

Variabel	*Person Correlation*	*Sig. (2-tailed)*	Ket.
Ransomware			
Pertanyaan 1	0,608	0,000	Valid
Pertanyaan 2	0,697	0,000	Valid
Pertanyaan 3	0,800	0,000	Valid
Pertanyaan 4	0,465	0,000	Valid
Pertanyaan 5	0,492	0,000	Valid
Pertanyaan 6	0,695	0,000	Valid
Pertanyaan 7	0,814	0,000	Valid
Pertanyaan 8	0,607	0,000	Valid
Pertanyaan 9	0,776	0,000	Valid
Pertanyaan 10	0,663	0,000	Valid
Phishing			
Pertanyaan 1	0,539	0,000	Valid
Pertanyaan 2	0,608	0,000	Valid
Pertanyaan 3	0,501	0,000	Valid
Pertanyaan 4	0,782	0,000	Valid
Pertanyaan 5	0,316	0,000	Valid
Pertanyaan 6	0,734	0,000	Valid
Pertanyaan 7	0,719	0,000	Valid
Pertanyaan 8	0,613	0,000	Valid
Pertanyaan 9	0,764	0,000	Valid
Pertanyaan 10	0,766	0,000	Valid
Tingkat Pemahaman Mahasiswa			
Pertanyaan 1	0,692	0,000	Valid
Pertanyaan 2	0,557	0,000	Valid
Pertanyaan 3	0,551	0,000	Valid
Pertanyaan 4	0,693	0,000	Valid
Pertanyaan 5	0,812	0,000	Valid

Pertanyaan 6	0,685	0,000	Valid
Pertanyaan 7	0,610	0,000	Valid
Pertanyaan 8	0,568	0,000	Valid
Pertanyaan 9	0,683	0,000	Valid
Pertanyaan 10	0,756	0,000	Valid

Sumber: Data diolah dari SPSS versi 17

Berdasarkan tabel 1. Hasil uji validitas semua item pertanyaan dalam kuesioner memiliki nilai *Person Correlation* yang positif dan signifikan pada tingkat signifikansi 0,000 (p < 0,05). Hal ini menunjukkan bahwa setiap pertanyaan dalam variabel "*Ransomware*", "*Phishing*", dan "Tingkat Pemahaman Mahasiswa" dinyatakan valid karena korelasi antar item dengan total skor variabel masing-masing cukup kuat. Nilai korelasi bervariasi, namun seluruhnya memenuhi syarat validitas, sehingga item-item dalam kuesioner dapat digunakan untuk mengukur masing-masing variabel secara tepat dan relevan. Validitas ini mengonfirmasi bahwa instrumen penelitian layak untuk digunakan dalam pengumpulan data.

2. Uji Reliabilitas

Tabel 2. Uji Reliabilitas

Variabel	*Cronbach's Alpha*	Ket.
Ransomware	0,854	*Reliable*
Phising	0,832	*Reliable*
Tingkat Pemahaman Mahasiswa	0,857	*Reliable*

Sumber: Data diolah dari SPSS versi 17

Berdasarkan tabel 2. Nilai *Cronbach's Alpha* untuk variabel *ransomware* adalah 0,854 atau 85,4%, yang lebih besar dari 0,60, sehingga dinyatakan reliabel. Nilai *Cronbach's Alpha* untuk variabel *phishing* sebesar 0,832 atau 83,2%, juga melampaui 0,60, sehingga dianggap reliabel. Sementara itu, nilai *Cronbach's Alpha* untuk variabel tingkat pemahaman mahasiswa adalah 0,857 atau 85,7%, yang lebih tinggi dari 0,60, sehingga hasilnya dinyatakan reliabel. Setiap variabel memiliki 10 item, menunjukkan uji reliabilitas dilakukan

melalui 10 indikator pertanyaan dalam kuesioner. Hal ini mengindikasikan indikator pertanyaan untuk variabel *ransomware, phishing*, dan tingkat pemahaman mahasiswa dinyatakan layak diuji, serta jawaban dari responden menunjukkan konsistensi.

3. Uji Normalitas

Tabel 3. Uji Normalitas

Asymp. Sig.	Keterangan
0,766	Terdistribusi normal

Sumber: Data diolah dari SPSS versi 17

Berdasarkan tabel 3. Uji normalitas menggunakan *One-Sample Kolmogorov-Smirnov* dilakukan dengan melihat nilai *sig*. >0,05, maka data terdistribusi normal (Ghozali, 2012). Berdasarkan tabel di atas dapat diketahui variabel tingkat pemahaman mahasiswa memiliki nilai *Asymp. Sig. (2-tailed)* 0,766 lebih besar dari *alpha* 0,05 yang berarti data terdistribusi normal.

4. Uji Multikolinearitas

Tabel 4. Uji Multikolinearitas

Model	*Collinearity Statistic*	
	Tolerance	VIF
X1	0,451	2,217
X2	0,451	2,217

Sumber: Data diolah dengan SPSS versi 17

Berdasarkan tabel 4. Hasil uji multikolinearitas terlihat bahwa nilai *Tolerance* untuk variabel *ransomware* sebesar 0,451 dan *phishing* sebesar 0,451, keduanya lebih besar dari 0,1. Sementara itu, nilai VIF untuk variabel *ransomware* sebesar 2,217 dan *phishing* sebesar 2,217, keduanya lebih kecil dari 10 sehingga dapat disimpulkan bahwa dalam penelitian ini tidak terjadi multikolinieritas.

5. Uji Regresi Linear Berganda

Tabel 5. Uji Regresi Linear Berganda

Model	*Unstandardized Coefficients*

	β
1 (*Constans)*	8.287
X1	0,348
X2	0,448

Sumber: Data diolah dari SPSS versi 17

Berdasarkan tabel 5. Hasil uji regresi linear berganda menunjukkan bahwa koefisien regresi untuk variabel X1 adalah 0,348, yang berarti setiap peningkatan satu unit pada X1 akan menyebabkan peningkatan sebesar 0,348 pada variabel terikat, dengan asumsi variabel X2 tetap konstan. Sementara itu, koefisien regresi untuk variabel X2 adalah 0,448, yang berarti setiap peningkatan satu unit pada X2 akan menyebabkan peningkatan sebesar 0,448 pada variabel terikat, dengan asumsi variabel X1 tetap konstan. Interpretasi ini menunjukkan adanya pengaruh positif dari kedua variabel independen terhadap variabel dependen.

6. Uji Koefisien Determinasi (R2)

Tabel 6. Uji Koefisien Determinasi

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,805	0,648	0,636	3,05300

Sumber: Data diolah dari SPSS versi 17

Berdasarkan tabel 6. Hasil uji R2 nilai *Adjusted R-Square* sebesar 0,648 menunjukkan bahwa 64,8% variasi data pada variabel tingkat pemahaman mahasiswa dapat dijelaskan oleh variabel *ransomware* dan *phishing*. Sedangkan 35,2% sisanya dipengaruhi oleh variabel-variabel lain yang tidak termasuk dalam penelitian ini. Dengan nilai *Adjusted R-Square* yang positif sebesar 0,648, dapat disimpulkan bahwa kontrol data dalam penelitian ini cukup baik.

7. Uji F

Tabel 7. Uji F

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1061,556	2	530,778	56,945	0,000
	Residual	577,890	62	9,321		
	Total	1639,446	64			

Sumber : Data diolah dari SPSS versi 17

Berdasarkan tabel 7. Hasil uji F menunjukkan bahwa F hitung sebesar 56,945 dengan nilai signifikansi sebesar 0,000. Nilai signifikansi lebih kecil dari pada tingkat signifikansi penelitian yaitu sebesar 0,05. Dapat disimpulkan bahwa *ransomware* dan *phishing* berpengaruh secara signifikan terhadap variabel tingkat pemahaman mahasiswa.

8. Uji t

Tabel 8. Uji t

Variabel Independen	t-tabel	t-hitung	Sig.
Konstanta	1,99601	2,932	0,005
X1	1,99601	3,293	0,002
X2	1,99601	4,377	0,000

Sumber: Data diolah dari SPSS versi 17

Berdasarkan tabel 8. Hasil uji t variabel X1 memiliki nilai t-hitung sebesar 3,293 dengan signifikansi 0,002, sementara variabel X2 memiliki t-hitung sebesar 4,377 dengan signifikansi 0,000. Kedua nilai signifikansi tersebut lebih kecil dari 0,05, yang menunjukkan bahwa X1 dan X2 secara individual berpengaruh signifikan terhadap Y.

Pengaruh *Ransomware* terhadap tingkat pemahaman mahasiswa

Ransomware tidak hanya memengaruhi dunia profesional dan industri tetapi juga berdampak signifikan pada ranah akademik, terutama dalam meningkatkan kesadaran mahasiswa terhadap isu-isu keamanan siber. Mahasiswa, sebagai generasi digital-native, sering terpapar teknologi dalam berbagai aspek kehidupan mereka, mulai dari komunikasi hingga pembelajaran. Dalam konteks ini, ancaman seperti ransomware menjadi pemantik yang efektif untuk memperluas pengetahuan mereka tentang keamanan siber. Berdasarkan hasil penelitian, t-hitung sebesar 3,293 dan nilai signifikansi 0,002 menunjukkan adanya hubungan yang kuat antara paparan ransomware dan tingkat pemahaman mahasiswa. Hal

ini berarti bahwa semakin banyak mahasiswa memahami bagaimana ransomware bekerja, semakin tinggi pula pemahaman mereka terhadap berbagai bentuk kejahatan siber lainnya. Dalam situasi tertentu, mahasiswa yang pernah mengalami atau menyaksikan insiden ransomware cenderung lebih proaktif dalam mencari informasi mengenai mekanisme pertahanan diri di dunia maya.

Fenomena ransomware telah mendorong integrasi materi keamanan siber ke dalam kurikulum pendidikan tinggi. Dalam beberapa program studi, misalnya ilmu komputer, teknologi informasi, dan bahkan hukum siber, pembahasan tentang ransomware sering dijadikan studi kasus untuk memberikan gambaran nyata kepada mahasiswa mengenai kompleksitas serangan siber. Paparan kasus nyata ini membuat mahasiswa lebih mudah memahami konsep-konsep seperti enkripsi data, serangan phishing, dan eksploitasi kerentanan perangkat lunak. Dari perspektif perilaku, ransomware juga meningkatkan kesadaran mahasiswa untuk lebih berhati-hati dalam menggunakan perangkat mereka. Sebagai contoh, mahasiswa menjadi lebih sadar akan pentingnya melakukan pencadangan data secara rutin, mengenali tanda-tanda file atau email mencurigakan, serta menghindari penggunaan perangkat lunak bajakan yang rentan terhadap serangan siber. Mereka juga lebih memahami peran penting perangkat lunak antivirus dan firewall dalam mencegah serangan ransomware. Fenomena ransomware turut memperluas wawasan mahasiswa mengenai dampak sosial dan ekonomi dari kejahatan siber. Mereka belajar bahwa serangan siber tidak hanya merugikan individu tetapi juga dapat berdampak besar pada organisasi, lembaga pemerintah, dan masyarakat luas. Pemahaman ini memicu mahasiswa untuk berpikir lebih kritis tentang bagaimana upaya kolektif, seperti regulasi keamanan siber, edukasi publik, dan pengembangan teknologi perlindungan, dapat membantu mengurangi risiko serangan ransomware di masa depan. Hasil penelitian ini memberikan landasan penting bagi institusi pendidikan untuk terus mengembangkan program pelatihan dan literasi siber bagi mahasiswa. Dengan meningkatkan pengetahuan mereka, mahasiswa tidak hanya mampu melindungi diri sendiri tetapi juga dapat berkontribusi dalam upaya pencegahan kejahatan siber secara lebih luas. Hal ini semakin relevan mengingat peran penting generasi muda dalam mendukung transformasi digital yang aman dan berkelanjutan.

Pengaruh *phishing* terhadap tingkat pemahaman mahasiswa

Penelitian ini menunjukkan bahwa phishing memiliki pengaruh positif terhadap tingkat pemahaman mahasiswa tentang kejahatan siber. Dengan nilai t-hitung sebesar 4,377 dan tingkat signifikansi 0,000 (di bawah ambang batas 0,05). Hasil ini memberikan bukti empiris yang kuat bahwa eksistensi phishing dapat meningkatkan kesadaran dan pengetahuan mahasiswa tentang berbagai bentuk ancaman di dunia maya. Phishing dilakukan melalui email atau pesan yang tampak resmi namun bertujuan mencuri informasi sensitif, seperti kata sandi atau data perbankan, memaksa mahasiswa untuk lebih waspada terhadap ancaman serupa. Paparan terhadap serangan phishing, baik secara langsung maupun tidak langsung, mendorong mahasiswa untuk lebih memahami pola-pola serangan tersebut. Mereka menjadi lebih paham cara mengenali tanda-tanda email atau pesan mencurigakan, seperti tautan yang tidak terpercaya, pengirim yang tidak dikenal, atau permintaan data pribadi secara tiba-tiba.

Hasil penelitian ini juga mencerminkan bahwa insiden phishing sering kali menjadi titik awal bagi mahasiswa untuk mempelajari lebih jauh tentang kejahatan siber secara umum. Dalam beberapa kasus, mahasiswa yang menjadi korban phishing atau menyaksikan insiden serupa cenderung lebih aktif mencari informasi mengenai langkah-langkah pencegahan, seperti penggunaan autentikasi dua faktor, pengelolaan kata sandi yang kuat, dan pengecekan keaslian situs web sebelum memberikan informasi pribadi.

Di lingkungan akademik, phishing sering kali digunakan sebagai studi kasus dalam pengajaran keamanan siber. Mahasiswa yang mempelajari topik ini di kelas atau melalui seminar, pelatihan, dan diskusi kelompok mendapatkan pemahaman yang lebih mendalam tentang teknik manipulasi sosial (social engineering) yang digunakan oleh pelaku phishing. Pengetahuan ini tidak hanya membantu mereka melindungi diri sendiri tetapi juga mempersiapkan mereka untuk memberikan edukasi kepada orang lain mengenai bahaya serangan phishing. Phishing memberikan dampak yang luas terhadap kesadaran mahasiswa tentang pentingnya literasi digital. Mereka mulai menyadari bahwa kepercayaan buta terhadap pesan elektronik dapat membawa risiko besar. Hal ini mendorong mereka untuk memanfaatkan teknologi keamanan, seperti filter spam, enkripsi email, dan perangkat lunak anti-malware. Selain itu, mahasiswa juga menjadi lebih peduli terhadap informasi yang

mereka bagikan di media sosial atau platform digital lainnya, mengingat data pribadi yang tersebar dapat dimanfaatkan oleh pelaku phishing untuk melancarkan serangan lebih lanjut. Dengan pemahaman yang lebih baik tentang phishing, mahasiswa dapat berkontribusi secara aktif dalam menciptakan ekosistem digital yang lebih aman. Upaya ini tidak hanya bermanfaat bagi individu tetapi juga memperkuat daya tahan masyarakat secara keseluruhan terhadap ancaman siber yang terus berkembang.

KESIMPULAN

Berdasarkan hasil penelitian ini, diketahui bahwa baik ransomware maupun phishing secara signifikan mempengaruhi tingkat pemahaman mahasiswa terhadap kejahatan siber, di mana kedua variabel tersebut menunjukkan pengaruh positif dan signifikan terhadap peningkatan pengetahuan dan kesadaran mahasiswa mengenai ancaman digital. Temuan ini mengindikasikan bahwa paparan terhadap serangan ransomware dan phishing mampu meningkatkan literasi keamanan siber di kalangan mahasiswa, sekaligus memperkuat kemampuan mereka dalam mengenali dan mengantisipasi serangan siber. Meski demikian, hasil penelitian ini memiliki keterbatasan, antara lain dari segi sampel yang relatif terbatas dan hanya berasal dari satu institusi pendidikan, sehingga generalisasi hasil ke populasi yang lebih luas perlu dilakukan dengan penelitian yang melibatkan berbagai latar belakang pendidikan dan wilayah geografis berbeda. Selain itu, variabel lain yang berpengaruh terhadap tingkat pemahaman mahasiswa seperti faktor pengalaman pribadi, tingkat pendidikan, dan akses terhadap edukasi keamanan siber belum diulas secara mendalam. Oleh karena itu, saran untuk penelitian selanjutnya adalah memperluas sampel dengan melibatkan berbagai institusi serta menambahkan variabel-variabel lain yang berperan dalam meningkatkan kesadaran dan pemahaman mahasiswa tentang kejahatan siber. Penelitian lanjutan juga disarankan untuk menggunakan pendekatan kualitatif guna memperoleh gambaran yang lebih mendalam mengenai faktor-faktor yang mempengaruhi tingkat literasi keamanan siber mahasiswa dan mengembangkan strategi edukasi yang lebih efektif dan kontekstual dalam menghadapi ancaman siber di masa depan.

DAFTAR PUSTAKA

Arifina, N., Sidik, F., & Sutanto, R. (2022). Strategi Pertahanan Siber Indonesia Di Pusat Pertahanan Siber Kementerian Pertahanan Republik Indonesia. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *9*, 2218–2227. https://doi.org/10.31604/jips.v9i6.2022.2218-2227

Arofah, N. R., & Priatnasari, Y. (2020). Internet Banking Dan Cyber Crime : Sebuah Studi Kasus Di Perbankan Nasional. In *Jurnal Pendidikan Akuntansi Indonesia* (Vol. 18, Issue 2).

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Elsevier Ltd*, *111*. https://doi.org/10.1016/j.cose.2021.102490

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Jurnal Hukum & Pembangunan*, *2*(2). https://doi.org/10.21143/telj.vol2.no2.1043

Caniago, K., & Sutabri, T. (2023). Tindak Kejahatan Phising Di Sektor Pelayanan Di Universitas Bina Insan Lubuklinggau. *Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)*, *8*. https://tunasbangsa.ac.id/ejurnal/index.php/jurasik/article/view/548/526

Dianita, Nurwahida, & Nurhayani. (2022). Proses Transaksi Pada Sistem Informasi Akuntansi Serta Implementasinya Pada Perbankan Syariah. *Asy-Syarikah, Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam*, *4*(1). http://journal.iaimsinjai.ac.id/index.php/asy-syarikah

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah : Identifikasi Ancaman Dan Tantangan Terkini. *Asy_Syarikah*, *5*(2). http://journal.uiad.ac.id/index.php/asy-syarikah

Fatimah, A., Pardede, A. K., & Kusmintarti, A. (2020). Jurnal Pendidikan Akuntansi Indonesia, Vol. 18, No. 1, Tahun 2020. *Jurnal Akuntansi Indonesia*, *16*(1), 44–51.

Fatkhur Rohmah, D. (2023). *Implementasi Manajamen Risiko Dalam Menghadapi Ancaman Phising Pada Bank Syariah Idonesia Kc Jakarta*.

Fenny Anita, & Tanujaya, K. (2023). Pengaruh Kejahatan Siber Terhadap Kinerja Organisasi Dengan Moderasi Kesadaran Keamanan Informasi. *Jurnal Ekuilnomi*, *5*(2), 266–275. https://doi.org/10.36985/ekuilnomi.v5i2.743

Gómez-Hernández, J. A., Sánchez-Fernández, R., & García-Teodoro, P. (2021). Inhibiting crypto-ransomware on windows platforms through a honeyfile-based approach with R-Locker. *IET Information Security*, *16*(1), 64–74. https://doi.org/10.1049/ise2.12042

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. *Bincang Sains Dan Teknologi*, *2*(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

Hidayat, W. M., Ramli, H., Mata Bulan Ikhram, P., Radif Ridhawi, A., Aisyah Mukhtar, N., & Junedy, R. (2023). Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa. *VOKATEX*. https://journal.diginus.id/index.php/VOKATEK/index

Kwarto, F., & Angsito, M. (2018). Pengaruh Cyber Crime Terhadap Cyber Security Compliance Di Sektor Keuangan. *Jurnal Akuntansi Bisnis*, *11*(2), 99–110. https://doi.org/10.30813/jab.v11i2.1382

Larasati, N. M., & Firdaus, R. (2024). Analisis Bahaya Serangan Ransomeware Terhadap Layanan Perbankan. *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *2*(4), 102–109. https://doi.org/10.61132/merkurius.v2i4.151

Rani Azura, S., Izari, & Galia Maharani, S. (2021). Kejahatan Elektronik Dalam Transasksi (Fraud Cyber Crime) Bursa Efek Indonesia PT DSFI. In *Jurnal Akuntansi & Keuangan Daerah* (Vol. 16, Issue 1).

Rompi, T., & Muaja, H. S. (2021). Tindak Kejahatan Siber Di Sektor Jasa Keuangan Dan Perbankan. *Lex Privatum*, *9*(4), 183–192.
https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/33358

Rosa, E., Sembiring, M., Nurbaiti, N., & Daulay, A. N. (2024). Pengaruh Ancaman Siber Ransomware dan Gangguan Sistem Layanan Mobile Banking Terhadap Kepercayaan Nasabah pada Bank BSI KCP Kisaran. *JURNAL MANAJEMEN PENDIDIKAN DAN ILMU SOSISAL (JMPIS)*, *5*(4). https://doi.org/10.38035/jmpis.v5i4

Sainuri Mubarak, A., Nur Insirat, M., & Nurul Lutfiya, M. (2024). Ransomware: Evolution, Classification, Attack Phase, Detection and Prevention. *Jurnal ITATS*. https://doi.org/10.31284/p.snestik.2024.5588

Saputra Gulo, A., Lasmadi, S., & Nawawi, K. (2020). Cyber Crime dalam Bentuk Phising Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik. *PAMPAS: Journal Of Criminal*, *1*. https://online-journal.unja.ac.id/Pampas/article/view/9574

Setia Buana, I. K., Novita Yasa, R., Girinoto, Setiawan, H., Budiarto Hadiprakoso, R., Kabetta, H., & Qomariasih, N. (2023). *Pembelajaran Anti Phising Melalui Media Edukasi Berupa Game Framework Di SMK Negeri 1 Negara* (Vol. 3). Jurnal WIDYA LAKSMI. https://jurnalwidyalaksmi.com/index.php/jwl/article/view/43

Shiring, B., Stanhope, C., Devito, H., Brigham, R., & Tschernov, L. (2024). *Adaptive Ransomware Detection Using Dynamic Encryption Pattern Analysis*. TechRxiv. https://doi.org/10.36227/techrxiv.173047783.31909733/v1

Simorangkir, A., Palangkaraya, U., Sihombing, H., Parhusip, J., Yos, J., Palangka, S., & Kalimantan, R. (2024). Ransomware pada Data PDN: Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber. *Jurnal Sains Student Research*, *2*(6). https://doi.org/10.61722/jssr.v2i6.2966

Surya Kusuma, R. (2023). Forensik Serangan Ransomware Ryuk pada Jaringan Cloud. In *Forensik Serangan Ransomware Ryuk pada Jaringan Cloud JURNAL MULTINETICS* (Vol. 9, Issue 2). https://doi.org/10.32722/multinetics.v9i2.5234

Syah, R. (2023). Strategi Kepolisian Dalam Pencegahan Kejahatan Phising Melalui Media Sosial Di Ruang Siber. *Jurnal Impresi Indonesia*, *2*(9), 864–870. https://doi.org/10.58344/jii.v2i9.3594

Tan, T., Sama, H., Wibowo, T., Wijaya, G., & Aboagye, O. E. (2024). Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam Cybersecurity Awareness among University Students in Batam City. *Jurnal Teknologi Dan Informasi (JATI)*, *14*. https://doi.org/10.34010/jati.v14i2

Ugbomah, N., Omede, N., & Ugochukwu, O. C. (2022). *Cybercrime: Predictive Impact On E-Commerce In Nigeria*. www.ijaar.org/sjssr

Vadila, N., & Pratama, A. R. (2021). *Analisis Kesadaran Keamanan Terhadap Ancaman Phishing*.

Wijaya, L., & Nurnawati, E. K. (2022). Analisis Kesadaran Mahasiswa Yogyakarta Tentang Phishing Pada Online Banking. *Jurnal Dinamika Informatika*, *11*(2).