



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SKRIPSI TERAPAN

PENGARUH KESADARAN KEAMANAN INFORMASI DAN *SECURITY HABITS* TERHADAP ANCAMAN SERANGAN SIBER PADA NASABAH BANK RAKYAT INDONESIA (BRI)



Disusun oleh:

Irene Septi Debora Sihotang / 2104421064

**PROGRAM STUDI KEUANGAN DAN PERBANKAN
PROGRAM PENDIDIKAN SARJANA TERAPAN
JURUSAN AKUNTANSI POLITEKNIK NEGERI JAKARTA
TAHUN 2025**



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SKRIPSI TERAPAN

PENGARUH KESADARAN KEAMANAN INFORMASI DAN *SECURITY HABITS* TERHADAP ANCAMAN SERANGAN SIBER PADA NASABAH BANK RAKYAT INDONESIA (BRI)



Disusun sebagai syarat untuk memperoleh gelar Sarjana Terapan
dari Politeknik Negeri Jakarta

Disusun oleh:

Irene Septi Debora Sihotang / 2104421064

**PROGRAM STUDI KEUANGAN DAN PERBANKAN
PROGRAM PENDIDIKAN SARJANA TERAPAN
JURUSAN AKUNTANSI POLITEKNIK NEGERI JAKARTA
TAHUN 2025**



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PERNYATAAN ORISINALITAS

Saya yang bertanda tangan di bawah ini:

Nama : Irene Septi Debora Sihotang

NIM : 2104421064

Program Studi : D4 Keuangan dan Perbankan

Jurusan : Akuntansi

Menyatakan bahwa yang dituliskan di dalam Skripsi ini adalah hasil karya saya sendiri bukan jiplakan (plagiasi) karya orang lain baik sebagian atau seluruhnya. Pendapat, gagasan, atau temuan orang lain yang terdapat di dalam Laporan Tugas akhir telah saya kutip dan saya rujuk sesuai dengan etika ilmiah. Demikian pernyataan ini saya buat dengan sebenar-benarnya.

**POLITEKNIK
NEGERI
JAKARTA**

Depok, 24 Juni 2025



Irene Septi Debora Sihotang

NIM. 2104421064



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi ini diajukan oleh:

Nama : Irene Septi Debora Sihotang
NIM : 2104421064
Program Studi : D4 Keuangan dan Perbankan
Judul Skripsi : **Pengaruh Kesadaran Keamanan Informasi dan
Security Habits terhadap Ancaman Serangan Siber
pada Nasabah Bank Rakyat Indonesia (BRI)**

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana S.Tr.M pada Program Studi D4 Keuangan dan Perbankan Jurusan Akuntansi Politeknik Negeri Jakarta.

DEWAN PENGUJI

Ketua Penguji : Dr. R. Elly Mirati S.E., M.M. ()
Anggota Penguji : Dr. Ida Nurhayati S.H., M.H. ()

DISAHKAN OLEH KETUA JURUSAN AKUNTANSI

Ditetapkan di : Depok
Tanggal : 30 Juni 2025

Ketua Jurusan Akuntansi

Dr. Sabar Warsini S.E., M.M.
NIP. 196404151990032002



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PERSETUJUAN SKRIPSI

Nama : Irene Septi Debora Sihotang
NIM : 2104421064
Jurusan / Program Studi : Akuntansi/Keuangan dan Perbankan Terapan
Judul Skripsi :

“Pengaruh Kesadaran Keamanan Informasi dan *Security Habits* terhadap Ancaman Serangan Siber pada Nasabah Bank Rakyat Indonesia (BRI)”

Disetujui oleh:
Pembimbing

Dr. Ida Nurhayati S.H., M.H.
NIP. 196305241997022001

**POLITEKNIK
NEGERI
JAKARTA**

Diketahui Oleh

KPS D4 Keuangan dan Perbankan

Heri Abrianto S.E., M.M.
NIP. 196510051997021001



KATA PENGANTAR

Puji serta syukur penulis panjatkan kepada ke hadirat Tuhan Yang Maha Esa atas segala limpahan berkat serta karunia-Nya sehingga penulis dapat menyelesaikan Skripsi dengan judul “PENGARUH KESADARAN KEAMANAN INFORMASI DAN SECURITY HABITS TERHADAP ANCAMAN SERANGAN SIBER PADA NASABAH BANK RAKYAT INDONESIA (BRI)”.

Adapun tujuan dari penyusunan skripsi ini adalah guna memenuhi salah satu syarat kelulusan dari program pendidikan sarjana terapan Keuangan dan Perbankan di Politeknik Negeri Jakarta. Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih kepada pihak-pihak yang telah terlibat dalam membantu, memberikan bimbingan, dan masukan, yaitu kepada:

1. Bapak Dr. Syamsurizal, S.E., M.M. selaku Direktur Politeknik Negeri Jakarta
2. Ibu Dr. Sabar Warsini, S.E., M.M. selaku Ketua Jurusan Akuntansi Politeknik Negeri Jakarta
3. Bapak Heri Abrianto, S.E., M.M. selaku Kepala Program Studi D4 Keuangan dan Perbankan
4. Ibu Ida Nurhayati selaku pembimbing Skripsi yang sudah sangat membantu penulis dalam memberikan masukan, pengarahan, serta meluangkan waktu dalam proses penyusunan skripsi terapan ini.
5. Seluruh staff pengajar jurusan Akuntansi Politeknik Negeri Jakarta yang telah memberikan ilmu yang bermanfaat selama penulis melaksanakan kegiatan perkuliahan di Politeknik Negeri Jakarta dan seluruh Staff Administrasi Jurusan Akuntansi Politeknik Negeri Jakarta yang telah membantu dalam proses penyusunan skripsi terapan ini.
6. Ibunda tercinta atas segala doa dan dukungan yang selalu diberikan, Abang-abang serta Kakak-kakak penulis yang selalu memberikan dukungan demi kelancaran penyusunan skripsi.
7. Almarhum Ayahanda tercinta, yang meskipun telah tiada, kasih sayang, nilai-nilai kehidupan, dan semangat juangnya senantiasa menjadi sumber inspirasi dan kekuatan bagi penulis dalam menempuh setiap langkah kehidupan, termasuk dalam menyelesaikan skripsi terapan ini.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

8. Oktafiano Reinaldi yang selalu menemani, serta memberikan dukungan dalam proses membuat skripsi terapan ini.
9. Indah Srimayanthi Lubis dan Nabila Syawalia Noor yang telah menjadi tempat penulis untuk berkeluh kesah, terima kasih atas seluruh bantuan, dan dukungan yang diberikan, sehingga penulis dapat menyelesaikan skripsi terapan ini.
10. Teman-teman seperjuangan diperkuliahan yang menemani dari awal hingga akhir perkuliahan dan teman-teman lainnya yang tidak bisa disebutkan satu persatu, terima kasih selalu membantu dan terima kasih untuk ilmu yang kita bagi bersama.
11. Seluruh pihak yang telah membantu penulis dalam mengerjakan skripsi terapan ini yang tidak dapat disebutkan satu persatu.

Dalam penyusunan skripsi terapan ini, penulis telah berupaya sebaik-baiknya agar dapat dipertanggungjawabkan. Namun, penulis menyadari bahwa dalam skripsi terapan ini masih banyak kekurangan. Maka dari itu, penulis menerima saran serta kritik yang bersifat membangun demi perbaikan di masa mendatang dari pembaca. Akhir kata penulis berharap semoga tugas yang telah diselesaikan oleh penulis ini dapat bermanfaat bagi rekan-rekan mahasiswa/i dan juga pembaca.

POLITEKNIK
NEGERI
JAKARTA



PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademis Politeknik Negeri Jakarta, saya yang bertanda tangan di bawah ini:

Nama : Irene Septi Debora Sihotang
NIM : 2104421064
Program Studi : D4 Keuangan dan Perbankan
Jurusan : Akuntansi
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul: **Pengaruh Kesadaran Keamanan Informasi dan *Security Habits* terhadap Ancaman Serangan Siber pada Nasabah Bank Rakyat Indonesia (BRI)**. Dengan hak bebas royalti non eksklusif ini Politeknik Negeri Jakarta berhak menyimpan, mengalih media atau mengformatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok

Pada Tanggal : 24 Juni 2025

Yang menyatakan

(Irene Septi Debora Sihotang)

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Irene Septi Debora Sihotang

Program Studi Keuangan dan Perbankan Terapan

Pengaruh Kesadaran Keamanan Informasi dan *Security Habits* terhadap Ancaman Serangan Siber pada Nasabah Bank Rakyat Indonesia (BRI)

ABSTRAK

Perkembangan layanan perbankan digital di Indonesia meningkat secara signifikan seiring kemajuan teknologi informasi, hal ini membawa dampak positif. Namun, seiring dengan kemajuan teknologi tersebut, risiko dan ancaman serangan siber terhadap nasabah turut mengalami peningkatan yang signifikan. Penelitian ini bertujuan untuk menganalisis pengaruh kesadaran keamanan informasi dan kebiasaan keamanan (*security habits*) terhadap ancaman serangan siber pada nasabah Bank Rakyat Indonesia (BRI). Penelitian menggunakan pendekatan kuantitatif dengan metode survei, melalui penyebaran kuesioner kepada 160 responden yang merupakan nasabah BRI yang berusia 30–70 tahun. Hasil penelitian menunjukkan bahwa: (1) kesadaran keamanan informasi berpengaruh positif dan signifikan terhadap ancaman serangan siber; (2) kebiasaan keamanan berpengaruh negatif dan tidak signifikan; dan (3) secara simultan, kedua variabel tersebut berpengaruh positif dan signifikan terhadap ancaman serangan siber. Temuan ini menggarisbawahi urgensi peningkatan literasi dan edukasi keamanan digital yang komprehensif dan berkelanjutan bagi pengguna layanan perbankan digital. Upaya mitigasi risiko siber perlu diarahkan pada penguatan kesadaran individu terhadap potensi ancaman, sebagai langkah strategis dalam mendorong perilaku protektif yang lebih efektif di era digital.

Kata kunci: Kesadaran Keamanan Informasi, *Security Habits*, Serangan Siber, Perbankan Digital, Nasabah BRI



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Irene Septi Debora Sihotang

Program Studi Keuangan dan Perbankan Terapan

The Influence of Information Security Awareness and Security Habits on Cyberattack Threats among Customers of Bank Rakyat Indonesia (BRI)

ABSTRACT

The development of digital banking services in Indonesia has increased significantly in line with advances in information technology, bringing various positive impacts. However, this progress is accompanied by a considerable rise in the risks and threats of cyberattacks targeting customers. This study aims to analyze the impact of information security awareness and security habits on cyberattack threats faced by Bank Rakyat Indonesia (BRI) Customers. A quantitative approach was employed using a survey method, through the distribution of questionnaires to 160 respondents who are BRI customers aged between 30 and 70 years. The findings indicate that: (1) information security awareness has a positive and significant influence on cyberattack threats; (2) security habits have a negative but insignificant influence; and (3) simultaneously, both independent variables have a positive and significant influence on cyberattack threats. These results underscore the urgency of enhancing comprehensive and sustainable digital security literacy and education among users of digital banking services. Cyber risk mitigation efforts should focus on strengthening individual awareness of potential threats as a strategic step in fostering more effective protective behavior in the digital era.

Keywords: Information Security Awareness, Security Habits, Cyberattack, Digital Banking, BRI Customers



DAFTAR ISI

SKRIPSI TERAPAN	i
SKRIPSI TERAPAN	ii
LEMBAR PERNYATAAN ORISINALITAS	iii
LEMBAR PENGESAHAN	iv
LEMBAR PERSETUJUAN SKRIPSI	v
KATA PENGANTAR.....	vi
ABSTRAK	ix
DAFTAR ISI.....	xi
DAFTAR GAMBAR.....	xiv
DAFTAR TABEL	xv
DAFTAR LAMPIRAN	xvi
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah Penelitian	8
1.3 Pertanyaan Penelitian	8
1.4 Tujuan Penelitian	9
1.5 Manfaat Penelitian.....	9
1.6 Sistematika Penulisan Skripsi	9
BAB II TINJAUAN PUSTAKA.....	12
2.1 Landasan Teori.....	12
2.1.1 Kesadaran Keamanan Informasi.....	Error! Bookmark not defined.
2.1.2 Security Habits.....	13
2.1.3 Protection Motivation Theory (PMT).....	14
2.1.3.1 Process of Threat Appraisal	14
2.1.3.2 Process of Coping Appraisal	Error! Bookmark not defined.
2.1.4 Serangan Siber	17
2.1.4.1 Jenis-jenis Serangan Siber.....	17
2.2 Penelitian Terdahulu.....	20
2.3 Kerangka Pemikiran	25
2.4 Hipotesis.....	26
BAB III METODOLOGI PENELITIAN	27
3.1 Jenis Penelitian.....	27
3.2 Objek Penelitian.....	27
3.3 Metode Pengambilan Sampel.....	28
3.3.1 Populasi.....	28
3.3.2 Sampel	28

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

3.4 Jenis dan Sumber Data Penelitian.....	29
3.5 Metode Pengumpulan Data Penelitian.....	29
3.5.1 Definisi Operasional Variabel	30
3.6 Metode Analisis data	32
3.6.1 Uji Instrumen Data	32
3.6.2 Uji Asumsi Klasik.....	34
3.6.3 Analisis Regresi Linear Berganda	36
3.6.4 Uji Hipotesis	36
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....	39
4.1 Hasil Penelitian	39
4.1.1 Kriteria Umum Responden.....	39
4.1.2 Gambaran Distribusi Item Pernyataan.....	45
4.1.3 Hasil Uji Instrumen Data	48
4.1.3.1 Uji Validitas	49
4.1.3.2 Uji Realibilitas	50
4.1.4 Hasil Uji Asumsi Klasik	50
4.1.4.1 Uji Normalitas.....	50
4.1.4.2 Uji Multikolinearitas.....	52
4.1.4.3 Uji Heteroskedastisitas	53
4.1.5 Analisis Regresi Linear Berganda	55
4.1.6 Uji Hipotesis	56
4.1.6.1 Uji T (Parsial).....	56
4.1.6.2 Uji F (Simultan)	58
4.1.6.3 Uji Koefisien Determinasi (Adjusted R ²)	58
4.2 Pembahasan Hasil Penelitian.....	59
4.2.1 Pengaruh Kesadaran Keamanan Informasi terhadap Ancaman Serangan Siber Pada Nasabah BRI.....	59
4.2.2 Pengaruh <i>Security Habits</i> terhadap Ancaman Serangan Siber Pada Nasabah BRI.....	61
4.2.3 Pengaruh Kesadaran Keamanan Informasi dan <i>Security Habits</i> terhadap Ancaman Serangan Siber Pada Nasabah BRI.....	63
BAB 5 PENUTUP.....	65
5.1 Simpulan	65
5.2 Saran	65
DAFTAR PUSTAKA.....	67
LAMPIRAN.....	70
Lampiran 1. 1 Kuesioner Penelitian	Error! Bookmark not defined.



© Hak Cipta milik Politeknik Negeri Jakarta

Lampiran 1. 2 Tabulasi Kuesioner Penelitian	73
Lampiran 1. 3 Hasil Uji Validitas dan Realibilitas	76
Lampiran 1. 4 Hasil Uji Asumsi Klasik	78
Lampiran 1. 5 Regresi Linear Berganda	80
Lampiran 1. 6 Hasil Uji Hipotesis	80
Lampiran 1. 7 Lembar Bimbingan	81



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



DAFTAR GAMBAR

Gambar 1. 1 Serangan Siber Tahun 2024	2
Gambar 1. 2 Grafik Laporan Abuse Domain	3
Gambar 1. 3 Data Korban Penipuan Digital Berdasarkan Generasi	4
Gambar 4. 1 Karakteristik Responden Berdasarkan Usia	40
Gambar 4. 2 Karakteristik Responden Berdasarkan Jenis Kelamin	41
Gambar 4. 3 Karakteristik Responden Berdasarkan Pendidikan Terakhir	42
Gambar 4. 4 Karakteristik Responden Berdasarkan Pekerjaan	44
Gambar 4. 5 Normal Probability P-P Plot.....	51
Gambar 4. 6 Hasil Uji One-Sample Kolmogorov Smirnov	52
Gambar 4. 7 Hasil Uji Multikolinearitas.....	53
Gambar 4. 8 Scatterplot.....	54
Gambar 4. 9 Hasil Uji Heteroskedastisitas	54
Gambar 4. 10 Hasil Uji Regresi Linear Berganda	55
Gambar 4. 11 Hasil Uji T (Parsial)	57
Gambar 4. 12 Hasil Uji F (Simultan).....	58
Gambar 4. 13 Hasil Uji Koefisien Determinasi (Adjusted R ²)	58

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



DAFTAR TABEL

Tabel 1. 1 Data Nasabah BRI Korban Serangan Siber Tahun 2023-2024.....	5
Tabel 2. 1 Penelitian Terdahulu	20
Tabel 3. 1 Skala Likert	30
Tabel 3. 2 Definisi Operasional Variabel.....	31
Tabel 4. 1 Karakteristik Responden Berdasarkan Usia.....	39
Tabel 4. 2 Karakteristik Responden Berdasarkan Jenis Kelamin	41
Tabel 4. 3 Karakteristik Responden Berdasarkan Pendidikan Terakhir	42
Tabel 4. 4 Karakteristik Responden Berdasarkan Pekerjaan	43
Tabel 4. 5 Gambaran Distribusi Item Kesadaran Keamanan Informasi (X1).....	46
Tabel 4. 6 Gambaran Distribusi Item Security Habits (X2).....	47
Tabel 4. 7 Gambaran Distribusi Item Serangan Siber (Y).....	48
Tabel 4. 8 Hasil Uji Validitas.....	49
Tabel 4. 9 Hasil Uji Realibilitas.....	50

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

**POLITEKNIK
NEGERI
JAKARTA**



DAFTAR LAMPIRAN

Lampiran 1. 1 Kuesioner Penelitian.....	Error! Bookmark not defined.
Lampiran 1. 2 Tabulasi Kuesioner Penelitian	73
Lampiran 1. 3 Hasil Uji Validitas dan Realibilitas	76
Lampiran 1. 4 Hasil Uji Asumsi Klasik	78
Lampiran 1. 5 Regresi Linear Berganda	80
Lampiran 1. 6 Hasil Uji Hipotesis	80
Lampiran 1. 7 Lembar Bimbingan.....	81



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB 1 PENDAHULUAN

1.1 Latar Belakang

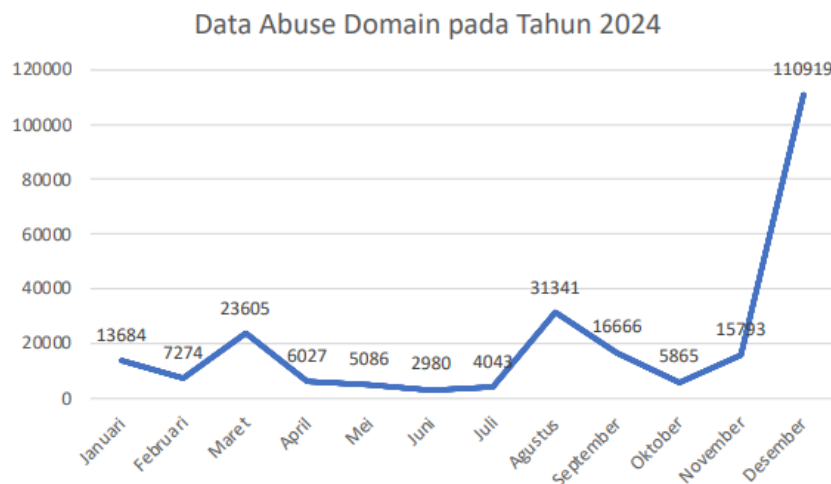
Layanan perbankan digital mulai berkembang, dimana seiring berkembangnya teknologi sehingga menciptakan kemudahan, disamping itu pula ada risiko yang akan dihadapi yaitu serangan siber, dalam Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber disebutkan bahwa “Serangan siber adalah segala bentuk perbuatan, perkataan, pemikiran baik yang dilakukan dengan sengaja maupun tidak sengaja oleh pihak mana pun, dengan motif dan tujuan apa pun, yang dilakukan di lokasi mana pun, yang didasarkan pada sistem elektronik atau muatannya (informasi) maupun peralatan yang sangat bergantung pada teknologi dan jaringan dalam skala apa pun, terhadap obyek vital maupun nonvital dalam lingkup militer dan nonmiliter, yang mengancam kedaulatan negara, keutuhan wilayah dan keselamatan bangsa.”(Kementrian Pertahanan Republik Indonesia, 2014). Serangan siber adalah perbuatan yang menyerang teknologi dan jaringan. Beberapa serangan siber pada perbankan adalah *Malware*, *Ransomware*, *Web Defacement*, *Denial of Service (DoS)* dan *Distributed Denial of Service (DDoS)*, *Phishing*, *Social engineering*, *Man-in-the-Middle (MitM)*, *Zero-Day Attack*, *Cyber Espionage*, *Supply Chain Attack*, *Credential Stuffing*.(OJK, 2024)



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Gambar 1. 1 Serangan Siber Tahun 2024
Sumber: Indonesia Anti-Phishing Data Exchange (IDADX)

Data *Abuse Domain* pada gambar diatas merupakan grafik yang dibuat oleh Indonesia Anti-Phishing Data Exchange (IDADX), *Abuse Domain* merupakan nama domain yang digunakan bertujuan untuk kejahatan atau merugikan pihaklain. Penggunaan istilah domain ini merupakan kegiatan penyalahgunaan yang dapat menimbulkan dampak negatif seperti kerugian secara finansial, kerugian data, dan masalah keamanan bagi individu dan suatu organisasi. Jenis konten yang dianggap sebagai *abuse domain* adalah *phishing*, *malware*, *spam*, judi online, pornografi, terorisme, SARA, dan lain sebagainya yang dapat merugikan pihak lain (IDADX, 2024). Data tersebut menunjukkan peningkatan yang signifikan selama tahun 2024, dan jika dibandingkan dengan tahun 2023 maka data tersebut mengalami peningkatan lebih dari 200%.

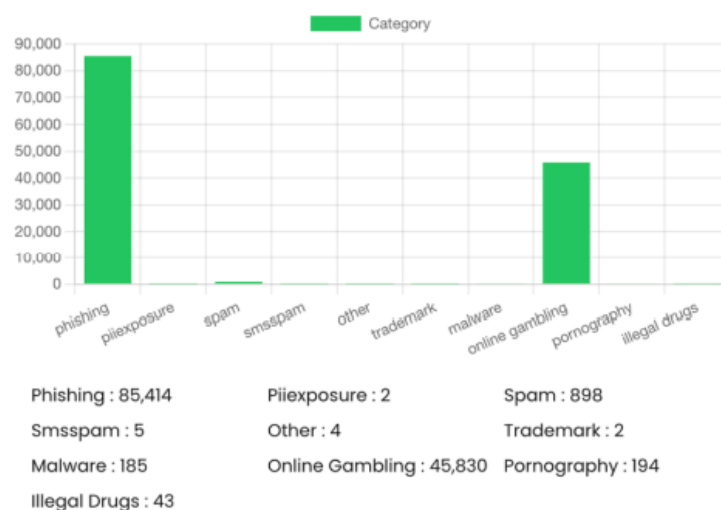


© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Abuse Data by Category



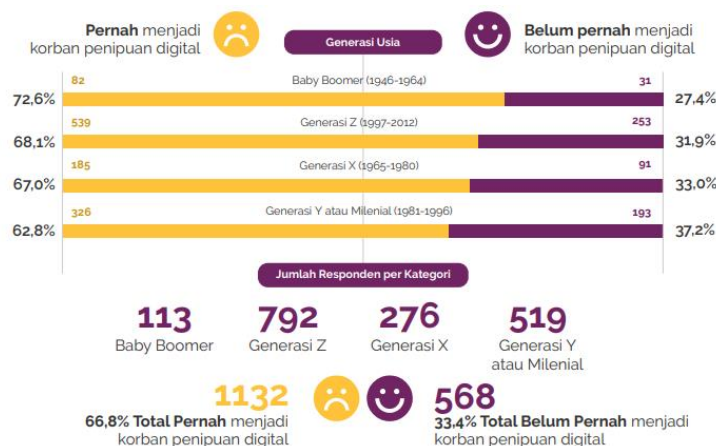
Gambar 1. 2 Grafik Laporan Abuse Domain
Sumber: Indonesia Anti-Phishing Data Exchange (IDADX)

Dari gambar 1.2 terdapat data berikut, dapat dilihat bahwa kategori *phising* merupakan laporan terbanyak, yang dimana *phising* adalah salah satu serangan siber yang merupakan tindakan yang bertujuan untuk memperoleh informasi pribadi seseorang seperti kata sandi dan informasi keuangan dengan menyamar sebagai web terpercaya, oleh karena itu bisa menjadi indikator bahwa keamanan internet di negara Indonesia masih lemah. Meningkatnya serangan siber dan data *breach* pada sektor perbankan dapat menimbulkan gangguan terhadap operasional layanan, kerugian finansial, serta mengancam kepentingan publik (Direktorat Operasi Keamanan Siber BSSN, 2023).



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Pada gambar 1.3 , dapat dilihat bahwa yang pernah menjadi korban penipuan digital yaitu pada generasi Z (12-28 Tahun) dengan jumlah 539 responden dari 792 responden, Generasi Y (24-39 Tahun) dengan jumlah 326 responden dari 519 responden, generasi X (40-55 Tahun) dengan jumlah 185 responden dari 276 responden, dan generasi *Baby Boomers* (61-79 Tahun) dengan jumlah 82 responden dari 113 responden (Kurnia et al., 2022, p. 80). Dari data tersebut tidak terdapat kepastian usia korban, dan jika dilihat dari perbandingan persentasenya, generasi yang paling tinggi adalah generasi *Baby Boomers* (61-79 Tahun), dan dari data tersebut menunjukkan bahwa diperlukannya kesadaran untuk menangkal penipuan-penipuan online atau serangan siber khususnya pada usia lanjut. Data tersebut merupakan riset secara umum, yang dimana pada penelitian ini penulis akan berfokus pada satu lembaga keuangan yaitu Bank Rakyat Indonesia (BRI).

Bank Rakyat Indonesia (BRI) merupakan bank milik pemerintah yang terbesar di Indonesia (BRI, 2025). Hingga akhir Desember 2024, BRI melayani lebih dari 70 juta nasabah di seluruh wilayah Indonesia. Jumlah pengguna BRImo mencapai 38,61 juta, meningkat 22,12% dibandingkan tahun sebelumnya dan total transaksi yang diproses melalui BRImo mencapai 4,34 miliar transaksi, tumbuh 40,54% (YoY), dengan nilai transaksi sebesar Rp5.596 triliun (Korporasi BRI, 2025). Pada tabel dibawah ini, terdapat beberapa kasus serangan siber yang terjadi



pada nasabah BRI.

Tabel 1. 1 Data Nasabah BRI Korban Serangan Siber Tahun 2023-2024

No	Nama, Usia, Pekerjaan Korban	Kasus	Deskripsi Kasus	Sumber
1	Silvia YAP, 52 Tahun, Pengusaha	<i>Social Engineering</i>	Pada Mei 2023, Seorang pengusaha di Malang bernama Silvia YAP merupakan nasabah prioritas BRI, melaporkan kehilangan saldo tabungannya sebesar Rp 1,4 Miliar, uang tersebut hilang usai membuka atau meng-klik undangan pernikahan dalam bentuk APK oleh pihak yang mengaku <i>Wedding Organizer</i> melalui sosial media <i>whatsapp</i> .	Metro TV (Faruq, 2023)
2	Serli Novitasari, 33 Tahun, Guru	<i>Social Engineering dan Phising</i>	Pada Oktober 2024, Serli N warga sumatera selatan yang merupakan nasabah pengguna <i>Mobile Banking</i> (BriMo) yang mengalami kehilangan uang ditabungannya, dan setelah diinvestigasi oleh BRI diduga nasabah menjadi korban penipuan online dengan modus pengiriman pesan singkat melalui aplikasi <i>Whatsapp</i> yang mengaku dari kantor instansi pemerintah yang memancing korban untuk memberikan data pribadi.	MSN (Tirto.id, 2025) dan Metro TV (Febriari, 2025)
3	Nyoman Werdiasa, 50 Tahun, Petani	Belum Diketahui, Diduga terkena serangan siber	Pada Agustus 2023, Nyoman Werdiasa seorang petani di Buleleng Bali yang melaporkan kehilangan uang tabungan di BRI senilai Rp 248 Juta, dan melaporkan pihak BRI ke Pengadilan Negeri Bali karena pihak BRI tidak mengganti kerugian Nyoman Werdiasa, karena pihak BRI merasa ini	Nusabali.com (Mao, 2023) dan Metro TV (Whisnu, 2023)

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Nama, Usia, Pekerjaan Korban	Kasus	Deskripsi Kasus	Sumber
			bukan kelalaian sistem BRI karena dari bukti transaksi nasabah adanya transfer ke rekening bank lain yang tidak dikenal, sedangkan Nyoman Werdiassa mengaku tidak pernah mengklik link dari pihak tidak dikenal, sehingga BRI hanya menghimbau nasabah BRI untuk tidak sembarang menginstal aplikasi dengan sumber tidak resmi karena bisa menyebabkan pencurian data atau informasi pribadi nasabah.	
4	Sri Fauzi, 62 Tahun, Seorang Ibu Lanjut Usia	<i>Malware</i>	Pada Desember 2024, Seorang wanita lanjut usia nasabah BRI bernama Sri Fauzi yang berusia 62 Tahun, mendatangi Porles Magetan untuk melaporkan kasus penipuan online yang berupa mengunduh aplikasi dari pelaku yang menggunakan modus iklan minyak goreng di Marketplace Sosial Media Facebook, dan pada saat bersamaan pelaku sambal menelepon Sri Fauzi dalih memberikan panduan, ini merupakan kasus serangan <i>Malware</i> dan <i>Social Engineering</i>	Regional.espos.id (Fawaid, 2024)
5	Riska, 33 Tahun, Pegawai Swasta	<i>Social Engineering</i>	Pada Mei 2024, Seorang warga Sidrap Sulawesi Selatan yang merupakan nasabah BRI bernama Riska melaporkan telah kehilangan saldo tabungannya di BRI, korban mengaku terkena modus ajakan berinvestasi menggunakan aplikasi Berna,a “Xendit”, korban	(Pena Rakyat, 2024)



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No	Nama, Usia, Pekerjaan Korban	Kasus	Deskripsi Kasus	Sumber
			merasa tidak sadar saat diminta untuk melakukan transfer ke penipu, yang dimana ini merupakan kasus <i>social engineering</i> .	

Sumber: Data diolah 2025

Pada Tabel 1.1 terdapat data-data nasabah BRI yang mengalami serangan siber, dan dapat dilihat bahwa adanya kasus-kasus penipuan online khususnya pada sektor perbankan ini menyebabkan kerugian besar secara finansial, dan jika dilihat dari data diatas, rata-rata usia nasabah BRI yang terkena serangan siber adalah rata-rata usia 30-70 tahun. Kondisi ini dimungkinkan terjadi akibat masih lemahnya sistem keamanan yang ada. Namun, seiring dengan meningkatnya ancaman siber, BRI secara aktif terus memperkuat infrastruktur keamanan digital untuk melindungi data nasabah. Berbagai langkah strategis telah diimplementasikan, antara lain penerapan teknologi keamanan digital mutakhir, pengembangan aplikasi yang terintegrasi dengan praktik keamanan sejak tahap pengembangan (*DevSecOps*), pemantauan keamanan teknologi informasi secara *real-time*, penanganan proaktif terhadap celah keamanan melalui manajemen kerentanan (*vulnerability management*), serta pembentukan Tim Tanggap Insiden Keamanan Komputer (*Computer Security Incident Response Team/CSIRT*) yang telah memperoleh sertifikasi dari BSSN. Selain itu, BRI juga mengadopsi *cybersecurity framework* berbasis standar NIST (*National Institute of Standards and Technology*) sebagai acuan dalam pengembangan keamanan digital, serta menerapkan sistem keamanan menyeluruh (*end-to-end security*) pada seluruh layanan perbankan digitalnya (BRI, 2024), juga dari beberapa lembaga keuangan khususnya BRI juga sudah memberikan imbauan dan edukasi kepada masyarakat terkait serangan siber, maka itu diperlukannya kesadaran akan ancaman serangan siber dan mengetahui cara untuk menghindari terkena serangan siber yang bertujuan untuk melindungi data dari nasabah sendiri. Karena sebagian besar yang terkena serangan siber adalah di usia rata-rata 30-70 tahun dan juga tidak menutup kemungkinan usia dibawah

Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

maupun diatas 30-70 tahun tidak terkena serangan siber, namun berdasarkan rata-rata usia nasabah BRI yang terkena serangan siber dan dikarenakan adanya keterbatasan waktu penelitian maka pada penelitian ini penulis akan berfokus pada nasabah BRI di usia 30-70 tahun.

Berdasarkan latar belakang tersebut penulis tertarik dan berkeinginan untuk melakukan penelitian yang berjudul **“Pengaruh Kesadaran Keamanan Informasi dan *Security Habits* Terhadap Ancaman Serangan Siber Pada Nasabah Bank Rakyat Indonesia (BRI)”**

1.2 Rumusan Masalah Penelitian

Berdasarkan penjelasan diatas, ditemukan adanya fenomena serangan siber yang masih marak terjadi, contohnya kasus *phising* yang paling banyak dilaporkan per 2024, dan kasus serangan siber di dunia perbankan juga masih banyak terjadi yang menyebabkan kerugian finansial, karena masih maraknya serangan siber khususnya pada nasabah bank, bank sendiri telah melakukan langkah-langkah keamanan untuk melindungi data nasabah disertai dengan adanya edukasi dan juga imbauan dari beberapa lembaga keuangan khususnya bank yang ditujukan kepada masyarakat, oleh karena itu perlunya ada kesadaran akan ancaman serangan dari sisi masyarakat sendiri, maka dari itu penelitian ini perlu dilakukan untuk mengetahui apakah masyarakat sudah memiliki kesadaran akan ancaman serangan siber sehingga dapat menghindari serangan siber yang menyebabkan kerugian khususnya secara finansial, oleh karena itu penelitian ini memasuki variabel yaitu kesadaran keamanan Informasi dan *security habits* untuk mengukur pengaruh terhadap ancaman serangan siber.

1.3 Pertanyaan Penelitian

Dengan dua variabel tersebut maka rumusan pertanyaan penelitian ini adalah:

1. Apakah kesadaran keamanan informasi berpengaruh terhadap ancaman serangan siber pada nasabah Bank Rakyat Indonesia?
2. Apakah *security habits* berpengaruh terhadap ancaman serangan siber pada nasabah Bank Rakyat Indonesia?



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

3. Apakah kesadaran keamanan informasi dan *security habits* tersebut berpengaruh simultan terhadap ancaman serangan siber pada nasabah Bank Rakyat Indonesia?

1.4 Tujuan Penelitian

Berdasarkan rumusan pertanyaan diatas, maka tujuan dari penelitian ini adalah:

1. Menguji dan menganalisis kesadaran keamanan informasi terhadap ancaman serangan siber pada nasabah Bank Rakyat Indonesia.
2. Menguji dan menganalisis *security habits* terhadap ancaman serangan siber pada nasabah Bank Rakyat Indonesia.
3. Menguji dan menganalisis kesadaran keamanan informasi dan *security habits* terhadap ancaman serangan siber pada nasabah Bank Rakyat Indonesia.

1.5 Manfaat Penelitian

Penelitian ini dibuat dengan tujuan:

1. Manfaat Praktis
Penelitian ini diharapkan dapat menjadi landasan untuk para pengguna layanan perbankan digital untuk memulai ataupun lebih menyadari akan ancaman serangan siber di perbankan, dan mengetahui cara untuk menghindarkan diri dari serangan siber melalui edukasi-edukasi maupun faktor-faktor yang mempengaruhi tingkat kesadaran.
2. Manfaat teoritis
Penelitian ini diharapkan dapat bermanfaat secara teoritis yaitu untuk memberikan landasan bagi para peneliti selanjutnya sebagai referensi dalam melakukan penelitian yang sejenis.

1.6 Sistematika Penulisan Skripsi

Penelitian ini akan terbagi dan terstruktur menjadi 5 (lima) bab. Berikut merupakan sistematika penulisan skripsi pada penelitian ini:



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I PENDAHULUAN

Bab ini menyajikan pembahasan awal yang mencakup latar belakang masalah, rumusan masalah, pertanyaan penelitian, tujuan penelitian, manfaat penelitian, serta sistematika penulisan skripsi. Bagian ini bertujuan untuk memberikan gambaran umum mengenai konteks penelitian, dasar pemikiran yang melatarbelakangi topik yang diangkat, serta arah dan kontribusi yang diharapkan dari penelitian yang dilakukan.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan landasan teori yang mendasari konseptual bagi variabel yang diteliti, disertai dengan tinjauan terhadap penelitian terdahulu yang relevan sebagai upaya untuk memperkuat konteks empiris. Selain itu, disajikan pula kerangka pemikiran yang menggambarkan alur logis hubungan antarvariabel dalam penelitian, serta perumusan hipotesis yang dikembangkan berdasarkan teori dan hasil penelitian sebelumnya. Bab ini bertujuan untuk membangun fondasi teoritis dan empiris yang kuat dalam mendukung proses analisis pada bab-bab selanjutnya.

BAB III METODE PENELITIAN

Bab ini membahas secara komprehensif mengenai metodologi penelitian yang digunakan dalam studi ini. Pembahasan mencakup jenis penelitian, objek penelitian, teknik penentuan sampel, jenis dan sumber data, serta metode pengumpulan data yang digunakan untuk memperoleh informasi yang relevan. Selain itu, bab ini juga menguraikan secara rinci teknik analisis data yang diterapkan untuk menguji hipotesis penelitian. Seluruh bagian dalam bab ini disusun guna memastikan bahwa penelitian dilakukan secara sistematis, terukur, dan dapat dipertanggungjawabkan secara ilmiah.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini menyajikan hasil penelitian yang diperoleh dari proses pengolahan dan analisis data yang telah dikumpulkan, serta dilanjutkan



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

dengan pembahasan yang mengacu pada rumusan masalah dan tujuan penelitian. Setiap temuan yang disampaikan dianalisis secara kritis dan dikaitkan dengan landasan teori serta hasil penelitian terdahulu. Bab ini bertujuan untuk menjelaskan sejauh mana data empiris mendukung hipotesis yang telah dirumuskan, serta memberikan interpretasi atas hasil yang diperoleh dalam konteks permasalahan yang diangkat dalam skripsi ini.

BAB V PENUTUP

Bab ini memuat kesimpulan yang disusun berdasarkan hasil analisis data dan pembahasan sebelumnya, serta merupakan jawaban atas pertanyaan penelitian yang telah dirumuskan. Selain itu, bab ini juga menyajikan saran yang bersifat konstruktif, baik untuk pengembangan penelitian selanjutnya maupun sebagai rekomendasi praktis bagi pihak-pihak yang relevan.

**POLITEKNIK
NEGERI
JAKARTA**



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB 5 PENUTUP

5.1 Simpulan

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan pada bab sebelumnya, maka dapat ditarik kesimpulan sebagai berikut:

1. Kesadaran Keamanan Informasi (X1) berpengaruh positif dan signifikan terhadap Ancaman Serangan Siber (Y). Hasil penelitian ini menunjukkan bahwa kesadaran keamanan informasi memiliki peran penting dalam melindungi nasabah BRI dari ancaman serangan siber. Ketika individu memiliki tingkat kesadaran yang tinggi seperti memahami risiko kebocoran data, merasa rentan terhadap ancaman digital, serta munculnya rasa takut jika informasi pribadi disalahgunakan mereka cenderung lebih waspada dan mampu mengambil langkah-langkah pencegahan secara aktif. Salah satu contohnya adalah kebiasaan memeriksa keaslian situs web sebelum memasukkan data pribadi.
2. *Security Habits* (X2) berpengaruh negatif dan tidak signifikan terhadap Ancaman Serangan Siber (Y). Penelitian ini menunjukkan bahwa meskipun sebagian besar responden memiliki kesadaran terhadap ancaman serangan siber, hal tersebut belum sepenuhnya diterjemahkan menjadi kebiasaan keamanan digital yang konsisten atau *security habits* yang kuat. Dengan kata lain, orang mungkin tahu apa yang seharusnya dilakukan untuk menjaga keamanan digital mereka, tetapi belum tentu benar-benar melakukannya dalam praktik sehari-hari.
3. Kesadaran Keamanan Informasi (X1) dan *security habits* (X2) berpengaruh secara simultan terhadap Ancaman Serangan Siber (Y). Penelitian ini menunjukkan bahwa kesadaran akan pentingnya keamanan informasi dan kebiasaan dalam menjaga keamanan digital ternyata sama-sama berperan dalam menghadapi ancaman serangan siber. Dalam konteks nasabah BRI, banyak yang sudah sadar bahwa dunia digital penuh risiko, tetapi tidak semuanya benar-benar mengubah kebiasaannya untuk lebih aman. Mereka tahu bahaya itu ada, tapi tidak selalu bertindak untuk menghindarinya.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

5.2 Saran

1. Bagi seluruh institusi perbankan di Indonesia:

Seluruh institusi perbankan di Indonesia termasuk BRI perlu terus secara efektif meningkatkan program edukasi dan literasi digital bagi nasabah melalui berbagai saluran komunikasi, khususnya terkait pentingnya kesadaran terhadap keamanan informasi dan langkah-langkah praktis menjaga keamanan digital. Bank perlu menyusun strategi keamanan berbasis pendekatan preventif, yang tidak hanya memperkuat sistem teknologi informasi, tetapi juga menanamkan kesadaran serta membentuk kebiasaan perilaku aman (*security habits*) pada pengguna layanan digital. Hal ini penting mengingat serangan siber tidak hanya bergantung pada sistem, tetapi juga pada perilaku pengguna dalam menjaga data dan informasi pribadi mereka. Penyuluhan dapat dilakukan melalui aplikasi mobile banking, email resmi, dan kampanye rutin di media sosial dengan menyasar kelompok usia rentan (30–70 tahun). Selain itu, institusi perbankan juga perlu memastikan bahwa seluruh karyawan mematuhi prinsip-prinsip etika profesi, menjaga kerahasiaan informasi nasabah, serta tidak menyalahgunakan akses internal terhadap data untuk kepentingan pribadi atau pihak lain, guna menciptakan lingkungan perbankan yang terpercaya dan aman secara menyeluruh.

2. Bagi Nasabah

Disarankan agar nasabah tidak hanya memiliki kesadaran, tetapi juga menerapkan perilaku protektif secara konsisten seperti menggunakan kata sandi yang kuat, memperbarui informasi keamanan secara berkala, dan tidak membagikan data pribadi kepada pihak yang tidak dikenal.

3. Bagi Peneliti Selanjutnya

Penelitian ini dapat diperluas dengan mempertimbangkan variabel lain seperti literasi digital, efikasi diri dalam teknologi, dan pengalaman sebelumnya menjadi korban kejahatan siber. Selain itu, analisis kualitatif dapat digunakan untuk mengeksplorasi lebih dalam mengapa *security habits* belum berpengaruh signifikan secara parsial.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR PUSTAKA

- Adam, A., & Juliadarma, M. (2024). *Sistem Informasi Manajemen: Tujuan Sistem Informasi Manajemen*. Akademia Pustaka.
- Adani, D. W., Nurhayati, I., & Mirati, R. E. (2024). SOSHUM Jurnal Sosial dan Humaniora [Journal of Social Sciences and Humanities] The Importance of Security Awareness in Combating Phishing Attacks : *Social Science and Medicine*, 14(3), 207–214.
- Alrawhani, E. M., Romli, A., & Al-Sharafi, M. A. (2025). Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach. *Journal of Open Innovation: Technology, Market, and Complexity*, 11(1), 100463. <https://doi.org/10.1016/j.joitmc.2024.100463>
- Alwanain, M. I. (2020). Phishing Awareness and Elderly Users in Social Media. *IJCSNS International Journal of Computer Science and Network Security*, 20(9), 114. <https://doi.org/10.22937/IJCSNS.2020.20.09.14>
- Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, 7(1), e06016. <https://doi.org/10.1016/j.heliyon.2021.e06016>
- Arpaci, I., & Aslan, O. (2023). Development of a Scale to Measure Cybercrime-Awareness on Social Media. *Journal of Computer Information Systems*, 63(3), 695–705. <https://doi.org/10.1080/08874417.2022.2101160>
- Binus. (2024). *Pengenalan Tentang Cyber Attack*. Binus University. <https://sis.binus.ac.id/2024/11/11/pengenalan-tentang-cyber-attack/>
- BPS. (2024). *Jumlah Penduduk Menurut Kelompok Umur dan Jenis Kelamin, 2024*. Badan Pusat Statistik. <https://www.bps.go.id/en/statistics-table/3/WVc0%2520MGEyMXBkVFUxY25KeE9HdDZkbTQzWkVkb1p6MDkjMw==/jumlah-penduduk-menurut-kelompok-umur-dan-jenis-kelamin-2023.html?year=2025>
- BRI. (2024). *Ini Langkah BRI Perkuat Keamanan Digital dari Serangan Siber*. BRI. https://bri.co.id/-tidak-diclick/-/asset_publisher/G3x3P8wG7JRn/content/ini-langkah-bri-perkuat-keamanan-digital-dari-serangan-siber
- BRI. (2025). *Tentang BRI*. BRI. <https://bri.co.id/tentang-bri>
- Cahyono, D., Fahrudin, R., Sinclair, A., Informatika, F. T., Info, A., Data, K., Banking, M., Multifactor, A., & Pengguna, E. (2024). *Pentingnya Edukasi dalam Mengatasi Keamanan Data Mobile Banking di Indonesia*. 3(1), 81–89.
- Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Employees Associated with Phishing Attacks. *Education and Information Technologies*, 27(4), 4729–4752. <https://doi.org/10.1007/s10639-021-10806-7>

Direktorat Operasi Keamanan Siber BSSN. (2023). *Imbauan Keamanan*. <https://bssn.go.id/imbauan-keamanan-modus-penipuan-menggunakan-undangan-pernikahan-elektronik-apk/>

Faruq, D. U. Al. (2023). *BRI Cabang Malang Tak Ganti Rugi Nasabah Kehilangan Rp1,4 Miliar karena Penipuan*. Metro TV. <https://www.metrotvnews.com/read/NLMCOGD9-bri-cabang-malang-tak-ganti-rugi-nasabah-kehilangan-rp1-4-miliar-karena-penipuan>

Fawaid, I. M. Z. (2024). *Nenek di Magetan Jadi Korban Penipuan Online, Saldo di Rekening Langsung Ludes*. Espos.Id.

Febriari, S. (2025). *BRI Investigasi Dugaan Hilangnya Dana Nasabah Senilai Rp402 Juta*. Metro TV. <https://www.metrotvnews.com/play/b3JCr4PY-bri-investigasi-dugaan-hilangnya-dana-nasabah-senilai-rp402-juta>

IDADX. (2024). *Laporan aktivitas abuse domain .id*.

Kemenkeu. (2020). *Prinsip Keamanan Informasi*. Kementerian Keuangan. <https://www.djkn.kemenkeu.go.id/kanwil-rsk/baca-artikel/13120/Keamanan-Informasi.html>

Kementerian Pertahanan Republik Indonesia. (2014). *Pedoman Pertahanan Siber*. *Pedoman Pertahanan Siber*, 5, 1–74.

Korporasi BRI. (2025). *Mudahkan Perjalanan Mudik Antarpulau, BRI Hadirkan Fitur Baru Pemesanan Tiket Kapal Lewat BRImo!* BRI. <https://www.bri.co.id/detail-news?title=mudahkan-perjalanan-mudik-antarpulau-bri-hadirkan-fitur-baru-pemesanan-tiket-kapal-lewat-brimo->

Kurnia, N., Rahayu, Wendratama, E., Monggilo, Z. M. Z., Damayanti, A., Angendari, D. A. D., Shafira, F. Q. A. I., & Desmalinda. (2022). *Penipuan Digital di Indonesia (Modus, Medium, dan Rekomendasi)* (Vol. 1). pr2media.

Mao. (2023). *Bank Plat Merah Digugat Nasabah di PN Singaraja, Menteri BUMN Jadi Ikut Turut Tergugat*. NusaBali .Com. <https://www.nusabali.com/index.php/berita/153371/bank-plat-merah-digugat-nasabah-di-pn-singaraja-menteri-bumn-jadi-ikut-turut-tergugat>

OJK. (2024). *Pedoman Keamanan Siber Bagi Penyelenggara Inovasi Teknologi Sektor Keuangan (ITSK) Pedoman Keamanan Siber*.

Riyanto, S., & Hatmawan, A. A. (2020). *Metode Riset Penelitian Kuantitatif Penelitian Di Bidang Manajemen, Teknik, Pendidikan, dan Eksperimen*. In *Deepublish* (p. 373). deepublish.

Sugiyono. (2020). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. In 2 (pp. III–434).



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- Suharso, P. (2012). *Metode Penelitian Kuantitatif Untuk Bisnis*. PT Index.
- Tirto.id. (2025). *Klarifikasi BRI soal Klaim Hilangnya Uang Nasabah di Palembang*. MSN. <https://www.msn.com/id-id/berita/other/klarifikasi-bri-soal-klaim-hilangnya-uang-nasabah-di-palembang/ar-AA1wdDkd>
- Walgito, B. (2010). *Pengantar Psikologi Umum*. Yogyakarta: ANDI.
- Whisnu. (2023). *Dana Nasabah BRI Milik Seorang Petani di Buleleng Senilai Rp248 Juta Raib*. Metro TV. <https://www.metrotvnews.com/read/Ky6CBgg6-dana-nasabah-bri-milik-seorang-petani-di-buleleng-senilai-rp248-juta-raib>
- Zhang, L., & McDowell, W. C. (2009). Am i really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce*, 8(3–4), 180–197. <https://doi.org/10.1080/15332860903467508>





Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LAMPIRAN

Lampiran 1. 1 Kuesioner Penelitian

Kepada yang terhormat,

Bapak/Ibu

Di tempat

Perkenalkan, saya Irene Septi Debora Sihotang, Mahasiswi Program Studi D4 Keuangan dan Perbankan dari Politeknik Negeri Jakarta, saat ini sedang melakukan penelitian untuk menyusun skripsi dengan judul:

"Pengaruh Kesadaran Keamanan Informasi dan Security Habits Terhadap Ancaman Serangan Siber Pada Nasabah Bank Rakyat Indonesia (BRI)."

Penelitian ini bertujuan untuk mengetahui bagaimana tingkat kesadaran keamanan informasi dan security habits para nasabah BRI guna mencegah terjadinya serangan siber.

Kuisioner ini dapat diisi apabila memenuhi kriteria sebagai berikut:

1. Nasabah Bank Rakyat Indonesia
2. Usia 30-70 Tahun

Saya mengharapkan kesediaan Bapak/Ibu untuk meluangkan waktu dalam mengisi kuesioner ini. Kuesioner ini bersifat anonim, dan seluruh data yang diberikan akan dijaga kerahasiaannya serta hanya digunakan untuk keperluan akademik. Terima Kasih

Hormat Saya, Peneliti

Irene Septi Debora Sihotang

1. Data diri Responden
 - a. Nama
 - b. Jenis Kelamin
 - c. Usia



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Pendidikan Terakhir

- e. Pekerjaan
2. Screening Questions
 - a. Apakah anda nasabah Bank Rakyat Indonesia? (Jika tidak, mohon untuk tidak melanjutkan kuisioner ini)
 - Ya
 - Tidak
 - b. Apakah anda berusia 30-70 Tahun (Jika tidak, mohon untuk tidak melanjutkan kuisioner ini)
 - Ya
 - Tidakdd

1. Pernyataan Kuersioner

No.	Variabel Kesadaran Keamanan Informasi (Proses Penilaian Ancaman)	Pilihan Jawaban				
		STS	TS	N	S	SS
Kerentanan Yang Dirasakan						
1	Saya menyadari bahwa sistem informasi yang saya gunakan berisiko terhadap serangan siber.					
2	Saya secara aktif menyadari adanya potensi risiko ketika menerima tautan atau file dari sumber yang tidak dikenal.					
3	Saya secara aktif untuk memeriksa keaslian situs web sebelum memasukkan informasi pribadi untuk menghindari serangan siber					
Timbulnya Rasa Takut						
4	Saya merasa khawatir akan kemungkinan terjadinya pencurian identitas melalui kebocoran data pribadi.					
5	Ketika menerima pesan atau tautan mencurigakan, saya merasa takut akan potensi kebocoran data					
6	Saya merasa tidak nyaman ketika diminta membagikan informasi pribadi secara daring, karena takut akan penyalahgunaan data					
No.	Variabel Security Habits (Proses Penilaian Penanggulangan)	Pilihan Jawaban				
		STS	TS	N	S	SS
Response Efficacy						
1	Saya percaya bahwa menggunakan kata sandi yang kuat dan unik untuk setiap akun dapat secara signifikan mengurangi risiko peretasan					
2	Saya percaya bahwa rutin mengganti kata sandi akun bank digital saya adalah strategi yang ampuh untuk menjaga keamanan informasi					
3	Saya percaya bahwa tidak membuka tautan atau lampiran dari sumber yang tidak dikenal dapat mencegah serangan siber					
Response Cost						
4	Saya rutin mengganti kata sandi pada akun bank digital saya					
5	Saya memperhatikan rekomendasi keamanan walaupun tindakan tersebut terasa terlalu teknis atau membingungkan					
6	Saya merasa memiliki cukup waktu atau kemampuan untuk memahami semua protokol keamanan digital yang disarankan					



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

No.	Variabel Ancaman Serangan Siber	Pilihan Jawaban				
		STS	TS	N	S	SS
Kesadaran Akan Serangan Siber						
1	Saya mengetahui jenis-jenis serangan siber					
2	Saya mengetahui bahwa serangan siber dalam perbankan dapat menyebabkan kerugian finansial yang signifikan					
3	Saya menyadari bahwa sektor perbankan merupakan salah satu target utama dari serangan siber					
Persepsi Probabilitas Terjadinya Serangan						
4	Saya memahami bahwa data nasabah seperti nomor rekening dan informasi kartu kredit sangat rentan terhadap pencurian oleh peretas					
5	Saya menyadari pentingnya tidak membagikan informasi login perbankan, seperti PIN atau OTP, kepada pihak mana pun					
6	Saya mengetahui bahwa pesan atau panggilan yang mengatasnamakan bank atau institusi resmi dapat menjadi bagian dari serangan phishing atau social engineering					





Lampiran 1. 2 Tabulasi Kuesioner Penelitian

Responden	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y	X1_1	X1_2	X1_3	X1_4	X1_5	X1_6	X1	X2_1	X2_2	X2_3	X2_4	X2_5	X2_6	X2
1	4	5	4	5	5	5	28	5	4	4	5	5	5	29	5	5	5	3	5	5	28
2	1	5	4	5	5	5	25	4	4	5	5	5	4	27	5	2	5	2	1	5	20
3	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
4	3	4	4	5	5	4	25	4	4	4	4	5	5	26	4	4	4	4	4	4	24
5	4	5	5	5	5	5	29	5	5	5	5	5	5	30	5	5	5	5	4	5	29
6	4	5	4	5	4	4	26	4	4	5	4	5	4	26	5	5	4	4	5	4	27
7	4	4	5	5	4	5	27	5	4	4	3	5	3	24	5	4	5	3	4	4	25
8	4	5	3	5	4	4	25	5	4	5	4	4	5	27	5	3	4	5	4	5	26
9	5	4	5	4	4	4	26	4	4	4	3	3	4	22	5	4	3	3	3	3	21
10	4	4	5	5	4	4	26	5	5	4	4	5	3	26	4	5	5	4	4	3	25
11	4	5	5	5	5	4	28	4	5	5	5	5	4	28	5	5	5	3	4	5	27
12	5	4	4	5	4	5	27	5	5	4	4	4	5	27	4	4	5	4	5	4	26
13	5	4	4	5	5	5	28	5	4	5	4	5	4	27	4	5	4	4	5	5	27
14	5	5	4	4	5	4	27	4	5	5	5	4	5	28	4	5	5	4	4	5	27
15	2	5	5	5	5	5	27	4	5	4	4	4	5	26	5	5	5	4	4	4	27
16	4	4	5	4	5	4	26	4	5	4	4	4	5	26	4	4	4	5	4	5	26
17	4	4	5	4	4	5	26	4	3	4	4	4	5	25	3	4	4	5	5	3	24
18	4	4	4	4	5	5	26	4	4	4	4	4	5	25	5	5	5	2	4	4	25
19	4	5	5	5	5	5	29	5	5	5	4	5	5	29	3	3	4	2	4	4	20
20	5	4	5	5	4	4	27	5	4	5	5	5	5	29	5	5	4	5	5	5	29
21	5	4	4	5	5	5	28	4	5	3	5	3	5	25	5	4	5	3	5	4	26
22	4	4	5	4	5	5	27	4	5	5	4	4	4	26	5	5	4	5	4	4	27
23	4	5	4	4	5	5	27	4	5	5	3	5	4	26	5	4	5	3	3	4	24
24	4	4	5	5	4	5	27	4	5	5	4	4	5	27	4	4	5	5	4	4	26
25	4	5	4	4	5	4	26	5	4	4	5	4	4	26	5	4	4	5	5	4	27
26	4	4	5	5	4	5	27	5	5	4	5	4	5	28	5	5	4	5	4	4	27
27	4	4	5	5	5	5	28	5	5	5	3	4	5	27	3	4	5	3	4	5	24
28	4	4	5	4	5	4	26	5	4	4	5	4	4	26	4	5	5	4	4	4	26
29	5	4	4	5	5	4	27	4	5	5	5	5	4	28	4	3	4	5	5	5	26
30	4	5	4	5	4	5	27	4	5	4	5	5	5	28	5	4	4	5	4	5	27
31	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
32	4	5	4	5	4	4	26	4	5	5	4	4	5	27	4	4	5	4	5	5	27
33	4	5	5	4	5	4	27	5	4	4	5	4	5	27	4	5	5	4	5	4	27
34	5	4	5	4	4	5	27	5	4	4	5	4	5	27	4	5	5	5	4	4	27
35	5	4	5	4	5	4	27	5	4	5	5	4	4	27	4	5	5	4	4	5	27
36	5	4	5	4	5	5	28	4	5	5	4	4	5	27	5	4	5	5	5	5	29
37	2	5	4	5	5	4	25	3	4	2	4	4	1	18	4	2	4	1	2	2	15
38	4	5	4	5	4	4	26	4	4	5	4	4	4	25	4	4	4	3	4	5	24
39	4	5	5	5	5	5	29	4	5	5	5	5	5	29	5	2	5	2	4	4	22
40	3	5	5	5	5	5	28	5	5	5	5	5	5	30	5	5	5	5	3	3	26
41	4	5	4	5	5	4	27	4	4	5	5	5	4	27	5	5	4	4	4	5	27
42	5	4	3	5	4	5	26	5	5	4	5	5	4	28	5	4	3	5	4	5	26
43	4	5	4	5	5	4	27	4	5	4	4	4	3	24	5	3	4	3	4	4	23
44	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
45	4	5	5	3	5	5	27	4	4	5	4	4	4	25	5	4	3	4	5	4	25
46	4	5	5	5	5	4	28	4	5	5	5	5	4	28	4	4	5	5	5	5	28
47	5	5	4	5	5	5	29	4	4	5	3	3	5	24	5	4	5	2	4	4	24
48	4	5	5	5	5	4	28	4	4	4	5	4	4	25	4	4	5	4	4	5	26
49	4	4	5	5	5	4	27	5	5	5	4	4	5	28	5	4	4	3	5	5	26
50	2	4	5	5	4	5	25	3	4	5	4	2	4	22	5	2	4	2	3	2	18



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Responden	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y	X1_1	X1_2	X1_3	X1_4	X1_5	X1_6	X1	X2_1	X2_2	X2_3	X2_4	X2_5	X2_6	X2
51	5	5	5	5	5	5	30	5	5	5	5	5	4	29	5	2	5	1	4	4	21
52	5	4	5	5	4	5	28	5	4	5	4	5	5	28	4	5	5	4	5	4	27
53	5	4	5	5	4	5	28	4	5	3	4	5	4	25	4	5	3	4	5	3	24
54	5	4	5	4	5	4	27	5	5	4	5	5	4	28	5	5	4	4	5	5	28
55	4	5	4	5	5	4	27	4	4	4	4	3	3	22	3	4	4	4	4	4	23
56	4	5	5	5	5	4	28	4	5	5	4	5	4	27	5	5	4	4	4	5	27
57	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
58	4	4	4	4	4	5	25	4	4	4	3	5	4	24	4	4	5	3	4	4	24
59	5	5	5	4	5	5	29	5	5	5	5	5	5	30	4	5	5	5	4	5	28
60	4	4	4	5	5	5	27	5	5	5	5	4	4	28	5	5	5	4	4	4	27
61	4	5	4	4	5	4	26	5	4	4	5	5	4	27	4	4	5	5	4	4	26
62	5	5	5	4	4	4	27	4	4	5	5	4	4	26	5	5	5	4	4	4	27
63	4	5	5	4	5	3	26	5	3	3	3	5	2	21	2	2	3	1	3	2	13
64	5	5	4	4	5	4	27	4	4	4	5	5	4	26	5	4	5	5	4	4	27
65	5	4	4	5	4	4	26	4	5	4	4	5	5	27	4	5	5	4	5	4	27
66	4	5	4	4	5	4	26	4	4	5	4	5	4	26	4	4	5	4	5	4	26
67	4	5	5	5	4	4	27	4	5	4	4	5	4	26	4	4	4	5	4	5	26
68	5	4	5	4	5	5	28	5	5	5	4	5	4	28	5	4	5	5	4	5	28
69	4	5	4	5	5	5	28	4	5	5	4	4	3	25	5	3	4	3	4	5	24
70	4	5	5	4	5	5	28	4	4	4	4	4	3	23	3	3	3	2	4	3	18
71	5	5	5	5	5	5	30	5	5	5	5	5	5	30	4	4	4	4	4	4	24
72	5	4	4	4	4	4	25	4	4	5	5	4	4	26	4	4	5	5	4	4	26
73	4	4	3	4	5	4	24	4	5	4	5	5	3	26	4	5	5	4	4	5	27
74	5	5	5	4	5	5	29	4	5	5	5	5	4	28	3	5	5	3	4	4	24
75	4	4	5	5	5	5	28	4	5	5	5	5	4	28	5	4	5	3	4	4	25
76	4	4	5	5	5	4	27	4	5	4	5	4	5	27	5	5	4	4	5	4	27
77	5	5	5	4	4	4	27	4	4	3	5	5	4	25	4	4	5	1	4	4	22
78	4	4	5	5	4	4	26	4	5	4	5	5	4	27	4	4	5	5	5	5	28
79	4	5	5	4	4	4	26	5	5	3	3	3	4	23	4	4	5	4	5	5	27
80	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
81	4	5	5	5	4	4	27	5	5	4	4	3	4	25	5	5	5	3	4	4	26
82	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
83	3	5	5	5	5	5	28	5	5	5	5	5	5	30	5	5	5	5	5	5	30
84	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
85	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
86	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
87	4	5	4	4	5	4	26	4	3	4	4	4	4	23	4	4	5	4	4	5	26
88	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
89	4	5	5	5	5	4	28	5	5	5	5	5	5	30	5	5	5	5	5	5	30
90	5	5	5	5	5	5	30	4	5	5	5	5	5	29	5	5	5	5	5	5	30
91	5	5	4	5	4	5	28	4	5	3	3	5	4	24	5	3	5	3	3	5	24
92	5	4	5	5	4	5	28	5	4	4	4	4	4	26	5	4	5	2	5	5	26
93	4	5	5	4	5	4	27	4	4	4	4	4	4	24	4	3	3	1	3	3	17
94	3	4	4	5	5	4	25	4	4	5	4	4	4	25	5	4	5	4	4	5	27
95	4	5	5	5	5	5	29	4	4	5	5	5	5	28	4	4	5	5	4	4	26
96	4	4	5	5	5	5	28	4	4	4	3	3	4	22	5	4	4	5	5	5	28
97	5	5	5	5	5	5	30	5	5	5	5	5	5	30	5	5	5	5	5	5	30
98	4	5	4	4	5	5	27	5	4	5	5	5	4	28	5	4	5	3	4	4	25
99	5	3	4	5	4	5	26	5	3	4	5	4	3	24	4	5	5	4	5	5	28
100	3	5	5	5	5	5	28	5	5	5	5	5	5	30	5	5	5	5	5	5	30



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Responden	Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y	X1_1	X1_2	X1_3	X1_4	X1_5	X1_6	X1	X2_1	X2_2	X2_3	X2_4	X2_5	X2_6	X2
101	5	5	4	4	5	4	27	5	5	4	4	3	4	25	5	4	4	5	4	4	26
102	4	4	5	2	5	5	25	5	4	5	5	5	5	29	5	5	5	5	5	5	30
103	4	5	4	4	4	4	25	4	4	4	4	5	5	26	5	1	5	1	3	3	18
104	3	4	4	5	5	5	26	4	5	5	4	4	4	26	5	3	4	2	3	4	21
105	4	5	5	4	5	5	28	5	4	4	5	5	5	28	4	3	5	1	3	3	19
106	1	5	5	5	5	5	26	5	4	5	3	4	1	22	4	3	4	1	5	1	18
107	5	4	4	5	5	4	27	5	5	4	4	5	5	28	5	4	5	3	5	5	27
108	5	5	4	5	4	4	27	5	5	4	4	5	5	28	5	2	5	2	5	5	24
109	4	5	5	4	4	3	25	5	3	4	5	4	4	25	5	3	4	4	4	5	25
110	4	5	5	3	4	5	26	4	5	4	3	4	5	25	4	5	5	5	4	5	28
111	5	5	4	5	5	5	29	2	5	4	4	4	5	24	5	4	5	5	4	4	27
112	4	5	5	4	5	4	27	5	5	4	5	4	4	27	5	4	5	5	4	3	26
113	5	4	4	3	5	4	25	5	4	5	5	4	4	27	5	4	5	4	4	4	26
114	2	4	4	5	5	5	25	3	4	5	2	2	4	20	5	2	4	2	4	4	21
115	3	5	4	5	5	4	26	4	2	5	4	4	4	23	5	2	4	2	5	5	23
116	4	5	5	5	5	4	28	4	3	3	5	4	4	23	4	3	5	4	4	3	23
117	4	5	4	4	5	5	27	5	4	4	5	5	4	27	5	4	4	4	5	4	26
118	4	5	3	4	5	4	25	4	5	4	5	4	5	27	5	4	3	4	5	3	24
119	5	4	5	4	5	4	27	4	4	5	5	4	5	27	4	4	5	3	4	4	24
120	5	4	4	5	4	5	27	5	5	5	5	4	4	28	5	5	4	5	5	5	29
121	4	5	4	4	5	5	27	4	2	5	4	4	4	23	4	4	5	4	4	4	25
122	4	5	4	5	5	4	27	4	5	5	4	4	5	27	4	2	5	2	4	4	21
123	4	4	5	5	5	5	28	5	5	4	5	4	5	28	5	4	5	5	5	4	28
124	5	5	4	5	5	4	28	4	5	4	5	4	5	27	4	5	4	4	4	5	26
125	4	5	4	4	5	5	27	4	5	5	4	5	4	27	5	4	5	2	4	5	25
126	4	5	5	4	5	5	28	4	4	4	5	5	5	27	4	4	5	5	4	4	26
127	4	5	5	4	4	4	26	4	4	5	4	5	5	27	5	4	4	3	5	4	25
128	4	4	4	5	5	5	27	4	5	5	5	4	3	26	4	4	5	5	4	5	27
129	5	5	4	5	5	4	28	4	5	5	5	5	5	29	3	4	5	3	4	3	22
130	5	4	4	5	4	4	26	5	4	4	5	4	4	26	4	5	5	4	5	4	27
131	4	4	5	4	5	4	26	4	4	5	4	4	5	26	4	5	5	4	5	4	27
132	3	4	5	4	4	5	25	4	5	5	4	5	4	27	5	4	5	5	4	5	28
133	4	5	5	5	5	5	29	5	5	5	5	5	5	30	5	4	5	2	4	4	24
134	5	4	5	5	4	4	27	5	4	5	5	4	5	28	5	4	5	5	4	5	28
135	4	4	4	5	5	5	27	5	5	5	5	5	5	30	5	2	5	2	5	5	24
136	4	3	5	5	5	4	26	3	5	5	4	4	5	26	5	5	4	3	4	5	26
137	4	4	5	4	4	4	25	5	4	5	4	5	4	27	4	4	4	5	4	4	25
138	5	5	4	4	5	4	27	5	5	4	4	4	5	27	5	5	4	4	4	5	27
139	5	5	5	5	5	5	30	5	5	4	5	5	5	29	5	4	5	4	5	4	27
140	4	5	4	5	4	5	27	5	3	4	5	3	4	24	5	4	4	3	4	4	24
141	4	4	5	5	4	5	27	4	4	5	4	5	5	27	5	4	5	5	4	5	28
142	3	5	5	4	5	5	27	5	5	5	4	5	5	29	4	4	4	3	4	4	23
143	5	4	5	5	5	4	28	5	4	5	4	4	5	27	4	5	5	5	5	4	28
144	5	5	4	5	5	4	28	4	5	5	4	4	4	26	4	4	5	2	4	5	24
145	4	5	5	5	5	5	29	5	5	5	5	5	5	30	5	4	4	3	4	4	24
146	4	5	4	4	5	4	26	4	4	5	5	4	5	27	4	4	5	4	4	4	25
147	5	5	4	5	4	5	28	5	5	5	5	4	5	29	5	5	4	5	5	4	28
148	5	5	5	5	5	5	30	5	5	5	5	5	5	30	3	3	4	3	5	5	23
149	4	4	5	4	5	4	26	5	4	4	5	5	4	27	5	5	4	5	4	4	27
150	5	4	4	5	4	4	26	4	4	5	5	4	4	26	4	4	5	4	4	5	26
151	3	4	5	5	5	5	27	4	4	5	5	4	4	26	5	4	4	3	4	5	25
152	4	5	5	4	5	5	28	5	5	5	5	5	4	29	5	1	5	1	5	5	22
153	5	5	4	5	5	4	28	4	4	5	4	4	5	26	4	3	5	2	4	4	22
154	4	4	5	4	5	5	27	4	4	5	4	5	5	27	4	5	5	4	5	5	28
155	4	5	4	4	5	4	26	5	4	4	5	4	5	27	4	5	4	5	4	5	27
156	5	5	4	5	5	3	27	5	3	5	3	4	5	25	5	3	5	2	4	5	24
157	4	4	5	5	5	4	27	5	5	4	5	4	5	28	5	4	4	5	5	5	28
158	5	4	5	5	4	3	26	5	5	4	4	3	4	25	4	5	4	4	5	4	26
159	3	5	3	5	5	4	25	5	4	4	4	3	4	24	5	4	5	5	4	4	27
160	5	4	3	4	5	4	25	5	4	5	5	4	5	28	5	4	5	4	5	5	28



Lampiran 1. 3 Hasil Uji Validitas dan Realibilitas

1. Hasil Uji Validitas

a. Kesadaran Keamanan Informasi (X1)

		Correlations									
		X1_1	X1_2	X1_3	X1_4	X1_5	X1_6	X1_7	X1_8	X1_9	X1
X1_1	Pearson Correlation	1	.469**	.595**	.313	.528**	.488**	.718**	.565**	.501**	.781**
	Sig. (2-tailed)		.005	<.001	.071	.001	.003	<.001	<.001	.003	<.001
	N	34	34	34	34	34	34	34	34	34	34
X1_2	Pearson Correlation	.469**	1	.270	.652**	.480**	.188	.490**	.583**	.376*	.691**
	Sig. (2-tailed)	.005		.123	<.001	.004	.288	.003	<.001	.028	<.001
	N	34	34	34	34	34	34	34	34	34	34
X1_3	Pearson Correlation	.595**	.270	1	.421*	.666**	.483**	.517**	.347*	.646**	.740**
	Sig. (2-tailed)	<.001	.123		.013	<.001	.004	.002	.044	<.001	<.001
	N	34	34	34	34	34	34	34	34	34	34
X1_4	Pearson Correlation	.313	.652**	.421*	1	.473**	.330	.398*	.479**	.493**	.696**
	Sig. (2-tailed)	.071	<.001	.013		.005	.057	.020	.004	.003	<.001
	N	34	34	34	34	34	34	34	34	34	34
X1_5	Pearson Correlation	.528**	.480**	.666**	.473**	1	.463**	.463**	.498**	.632**	.782**
	Sig. (2-tailed)	.001	.004	<.001	.005		.006	.006	.003	<.001	<.001
	N	34	34	34	34	34	34	34	34	34	34
X1_6	Pearson Correlation	.488**	.188	.483**	.330	.463**	1	.444**	.425*	.494**	.638**
	Sig. (2-tailed)	.003	.288	.004	.057	.006		.009	.012	.003	<.001
	N	34	34	34	34	34	34	34	34	34	34
X1_7	Pearson Correlation	.718**	.490**	.517**	.398*	.463**	.444**	1	.624**	.647**	.793**
	Sig. (2-tailed)	<.001	.003	.002	.020	.006	.009		<.001	<.001	<.001
	N	34	34	34	34	34	34	34	34	34	34
X1_8	Pearson Correlation	.565**	.583**	.347*	.479**	.498**	.425*	.624**	1	.483**	.748**
	Sig. (2-tailed)	<.001	<.001	.044	.004	.003	.012	<.001		.004	<.001
	N	34	34	34	34	34	34	34	34	34	34
X1_9	Pearson Correlation	.501**	.376*	.646**	.493**	.632**	.494**	.647**	.483**	1	.784**
	Sig. (2-tailed)	.003	.028	<.001	.003	<.001	.003	<.001	.004		<.001
	N	34	34	34	34	34	34	34	34	34	34
X1	Pearson Correlation	.781**	.691**	.740**	.696**	.782**	.638**	.793**	.748**	.784**	1
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	
	N	34	34	34	34	34	34	34	34	34	34

** Correlation is significant at the 0.01 level (2-tailed).

* Correlation is significant at the 0.05 level (2-tailed).

b. Security Habits (X2)

		Correlations						
		X2_1	X2_2	X2_3	X2_4	X2_5	X2_6	X2
X2_1	Pearson Correlation	1	.378*	.459**	.080	.273	.467**	.613**
	Sig. (2-tailed)		.028	.006	.651	.118	.005	<.001
	N	34	34	34	34	34	34	34
X2_2	Pearson Correlation	.378*	1	.361*	.263	.246	.323	.626**
	Sig. (2-tailed)	.028		.036	.133	.161	.062	<.001
	N	34	34	34	34	34	34	34
X2_3	Pearson Correlation	.459**	.361*	1	.222	.145	.088	.578**
	Sig. (2-tailed)	.006	.036		.207	.412	.620	<.001
	N	34	34	34	34	34	34	34
X2_4	Pearson Correlation	.080	.263	.222	1	.497**	.281	.695**
	Sig. (2-tailed)	.651	.133	.207		.003	.107	<.001
	N	34	34	34	34	34	34	34
X2_5	Pearson Correlation	.273	.246	.145	.497**	1	.492**	.705**
	Sig. (2-tailed)	.118	.161	.412	.003		.003	<.001
	N	34	34	34	34	34	34	34
X2_6	Pearson Correlation	.467**	.323	.088	.281	.492**	1	.643**
	Sig. (2-tailed)	.005	.062	.620	.107	.003		<.001
	N	34	34	34	34	34	34	34
X2	Pearson Correlation	.613**	.626**	.578**	.695**	.705**	.643**	1
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	<.001	<.001	
	N	34	34	34	34	34	34	34

* Correlation is significant at the 0.05 level (2-tailed).

** Correlation is significant at the 0.01 level (2-tailed).

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
- a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
- b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



c. Serangan Siber (Y)

		Correlations								
		Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y
Y_1	Pearson Correlation	1	.215	.447**	.396*	.419*	.504**	.448**	.398*	.673**
	Sig. (2-tailed)		.221	.008	.021	.014	.002	.008	.020	<.001
	N	34	34	34	34	34	34	34	34	34
Y_2	Pearson Correlation	.215	1	.389*	.267	.463**	.429*	.412*	.395*	.604**
	Sig. (2-tailed)	.221		.023	.126	.006	.011	.015	.021	<.001
	N	34	34	34	34	34	34	34	34	34
Y_3	Pearson Correlation	.447**	.389*	1	.347*	.259	.217	.522**	.408*	.605**
	Sig. (2-tailed)	.008	.023		.045	.139	.217	.002	.017	<.001
	N	34	34	34	34	34	34	34	34	34
Y_4	Pearson Correlation	.396*	.267	.347*	1	.569**	.298	.482**	.676**	.722**
	Sig. (2-tailed)	.021	.126	.045		<.001	.087	.004	<.001	<.001
	N	34	34	34	34	34	34	34	34	34
Y_5	Pearson Correlation	.419*	.463**	.259	.569**	1	.664**	.611**	.387*	.776**
	Sig. (2-tailed)	.014	.006	.139	<.001		<.001	<.001	.024	<.001
	N	34	34	34	34	34	34	34	34	34
Y_6	Pearson Correlation	.504**	.429*	.217	.298	.664**	1	.643**	.412*	.737**
	Sig. (2-tailed)	.002	.011	.217	.087	<.001		<.001	.015	<.001
	N	34	34	34	34	34	34	34	34	34
Y_7	Pearson Correlation	.448**	.412*	.522**	.482**	.611**	.643**	1	.610**	.828**
	Sig. (2-tailed)	.008	.015	.002	.004	<.001	<.001		<.001	<.001
	N	34	34	34	34	34	34	34	34	34
Y_8	Pearson Correlation	.398*	.395*	.408*	.676**	.387*	.412*	.610**	1	.757**
	Sig. (2-tailed)	.020	.021	.017	<.001	.024	.015	<.001		<.001
	N	34	34	34	34	34	34	34	34	34
Y	Pearson Correlation	.673**	.604**	.605**	.722**	.776**	.737**	.828**	.757**	1
	Sig. (2-tailed)	<.001	<.001	<.001	<.001	<.001	<.001	<.001	<.001	
	N	34	34	34	34	34	34	34	34	34

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

2. Hasil Uji Realibilitas

a. Kesadaran Keamanan Informasi (X1)

Reliability Statistics

Cronbach's Alpha	N of Items
.895	9

b. Security Habits (X2)

Reliability Statistics

Cronbach's Alpha	N of Items
.703	6

c. Serangan Siber (Y)

Reliability Statistics

Cronbach's Alpha	N of Items
.895	9

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :

a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penerbitan karya ilmiah, penerbitan laporan, penerbitan kritik atau tinjauan suatu masalah.

b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta

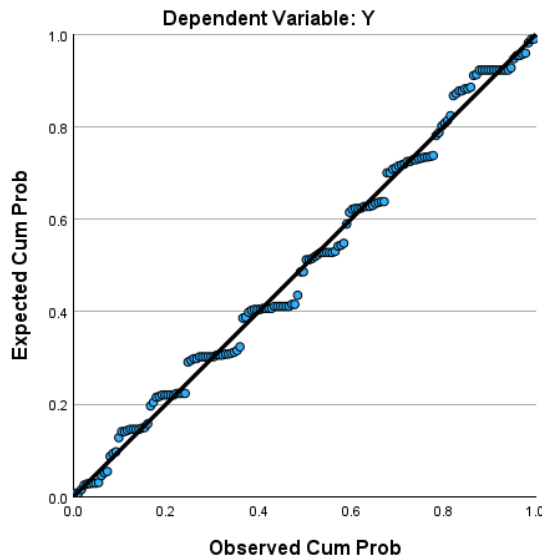
2. Dilarang mengutip dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Lampiran 1. 4 Hasil Uji Asumsi Klasik

1. Uji Normalitas

Normal P-P Plot of Regression Standardized Residual



One-Sample Kolmogorov-Smirnov Test

		Unstandardized Residual
N		160
Normal Parameters ^{a, b}	Mean	.0000000
	Std. Deviation	1.19415939
Most Extreme Differences	Absolute	.066
	Positive	.066
	Negative	-.050
Test Statistic		.066
Asymp. Sig. (2-tailed) ^c		.085
Monte Carlo Sig. (2-tailed) ^d	Sig.	.089
	99% Confidence Interval	
	Lower Bound	.081
	Upper Bound	.096

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

d. Lilliefors' method based on 10000 Monte Carlo samples with starting seed 299883525.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



2. Uji Multikolinearitas

Coefficients^a

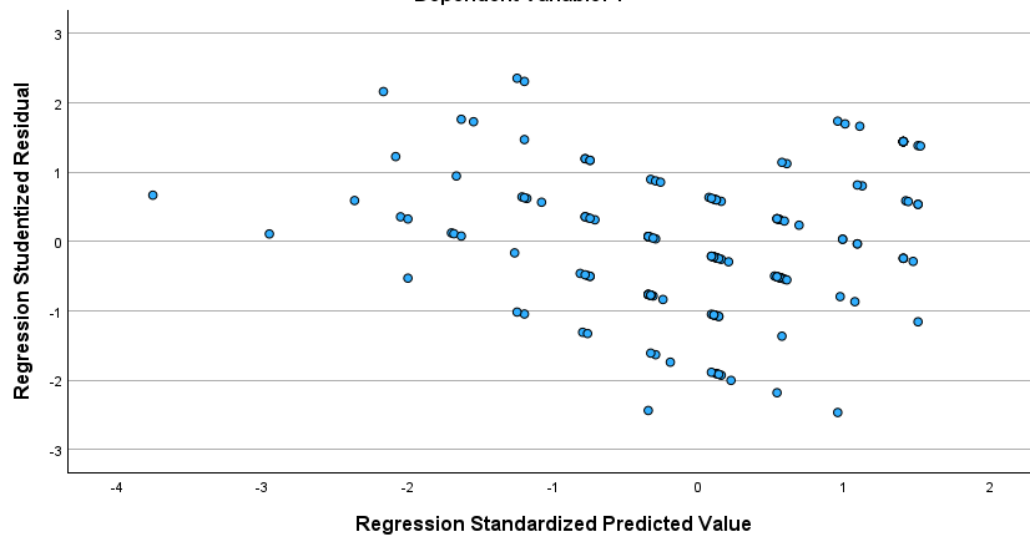
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	18.084	1.146		15.775	<.,001		
	X1	.353	.050	.563	7.105	<.,001	.708	1.412
	X2	-.013	.037	-.028	-.356	.722	.708	1.412

a. Dependent Variable: Y

3. Uji Heteroskedastisitas

Scatterplot

Dependent Variable: Y



Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.293	.680		.431	.667
	X1	.016	.029	.051	.544	.587
	X2	.009	.022	.040	.418	.676

a. Dependent Variable: ABS_RES

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Lampiran 1. 5 Regresi Linear Berganda

Coefficients ^a							
Model		Unstandardized Coefficients B	Std. Error	Standardized Coefficients Beta	t	Sig.	Collinearity Statistics Tolerance VIF
1	(Constant)	18.084	1.146		15.775	<,001	
	X1	.353	.050	.563	7.105	<,001	.708 1.412
	X2	-.013	.037	-.028	-.356	.722	.708 1.412

a. Dependent Variable: Y

Lampiran 1. 6 Hasil Uji Hipotesis

1. Hasil Uji T (Parsial)

Coefficients ^a							
Model		Unstandardized Coefficients B	Std. Error	Standardized Coefficients Beta	t	Sig.	Collinearity Statistics Tolerance VIF
1	(Constant)	18.084	1.146		15.775	<,001	
	X1	.353	.050	.563	7.105	<,001	.708 1.412
	X2	-.013	.037	-.028	-.356	.722	.708 1.412

a. Dependent Variable: Y

2. Hasil Uji F (Simultan)

ANOVA ^a					
Model		Sum of Squares	df	Mean Square	F Sig.
1	Regression	97.638	2	48.819	33.804 <,001 ^b
	Residual	226.737	157	1.444	
	Total	324.375	159		

a. Dependent Variable: Y

b. Predictors: (Constant), X2, X1

3. Uji Koefisien Determinasi (R^2)

Model Summary ^b				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.549 ^a	.301	.292	1.20174

a. Predictors: (Constant), X2, X1

b. Dependent Variable: Y



Lampiran 1. 7 Lembar Bimbingan



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
POLITEKNIK NEGERI JAKARTA
JURUSAN AKUNTANSI
Jl. Prof. Dr. G. A. Siwabessy, Kampus UI, Depok, 16425
Telepon (021) 7863534, 7864827, 786426, 7270042, 7270035
Fax (021) 7270034, (021) 7270036 Hunting
Laman: <http://www.pnj.ac.id> e-pos: humas@pnj.ac.id

LEMBAR BIMBINGAN

- | | |
|---------------------|--|
| 1. Nama Mahasiswa | : Irene Septi Debora Sihotang |
| 2. NIM | : 2104421064 |
| 3. Program Studi | : D4 Keuangan dan Perbankan |
| 4. Judul Skripsi | : Pengaruh Kesadaran Keamanan Informasi dan <i>Security Habits</i> Terhadap Ancaman Serangan Siber |
| 5. Dosen Pembimbing | : Dr. Ida Nurhayati, S.H., M.H. |

No.	Tanggal	Materi Bimbingan	TTD Dosen Pembimbing
1.	Sabtu, 22/2/25	Rancangan /outline skripsi	
2.	Senin, 3/3/25	BAB 1 dan Revisi	
3.	Rabu, 9/4/25	BAB 1 dan BAB 2 (Revisi)	
4.	Senin, 14/4/25	BAB 2 dan BAB 3	
5.	Rabu, 16/4/25	ACC BAB 2 dan BAB 3	
6.	Jumat, 16/5/25	Revisi sempro	
7.	Senin, 26/5/25	Bimbingan olah data	
8.	Senin, 24/6/25	Bimbingan dan ACC BAB 4 dan 5	

Menyetujui,
KPS D4 Keuangan dan Perbankan
Depok,

Heri Abrianto, S.E., M.M.
NIP. 196510051997021001

- Hak Cipta :**
1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
 2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta