

SKRIPSI

PENGARUH LITERASI DAN KEAMANAN DATA PRIBADI TERHADAP KEWASPADAAN TERHADAP PENIPUAN DIGITAL PADA NASABAH BANK ACEH SYARIAH DI KOTA BANDA ACEH



Disusun Oleh :

**RIFQI ALDIAN
NIM. 220603092**

**PRODI PERBANKAN SYARIAH
FAKULTAS EKONOMI DAN BISNIS ISLAM
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA
ACEH
TAHUN 2026 M/ 1448**

PENYATAAN KEASLIAN KARYA ILMIAH

Yang bertandatangan di bawah ini

Nama : Rifqi Aldian

NIM : 220603092

Program Studi : Perbankan Syariah

Fakultas : Ekonomi Dan Bisnis Islam

Dengan ini menyatakan bahwa dalam penelitian skripsi ini, saya:

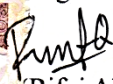
1. *Tidak menggunakan ide orang lain tanpa mampu mengembangkan dan bertanggungjawabkan.*
2. *Tidak melakukan plagiasi terhadap nasakah karya orang lain.*
3. *Tidak menggunakan karya orang lain tanpa menyebutkan sumber asli atau tanpa izin pemilik karya*
4. *Tidak melakukan manipulasi dan pemalsuan data.*
5. *Mengerjakan sendiri karya ini dan mampu bertanggungjawab atas karya ini.*

Bila dikemudian hari ada tuntutan dari pihak lain atas karya saya, dan telah melalui pembuktian yang dapat dipertanggungjawabkan dan ternyata memang ditemukan bukti bahwa saya telah melanggar pernyataan ini, maka saya siap untuk dicabut gelar akademik saya atau diberikan sanksi lain berdasarkan aturan yang berlaku di Fakultas Ekonomi dan Bisnis islam UIN Ar-Raniry Banda Aceh.

Demikian pernyataan ini saya buat dengan sesungguhnya.

Banda Aceh 26 agustus 2026

Yang Menyatakan


(Rifqi Aldian)



PERSETUJUAN SIDANG MUNAQASYAH SKRIPSI

**PENGARUH LITERASI DAN KEAMANAN DATA PRIBADI
TERHADAP KEWASPADAAN TERHADAP PENIPUAN DIGITAL
PADA NASABAH BANK ACEH SYARIAH DI KOTA BANDA
ACEH**

Disusun Oleh:

Rifqi Aldian

NIM: 220603092

Disetujui untuk disidangkan dan dinyatakan bahwa isi dan formatnya
telah memenuhi syarat penyelesaian studi pada Program Studi
Perbankan Syariah Fakultas Ekonomi dan Bisnis Islam
Universitas Islam Negeri Ar-Raniry Banda Aceh

Pembimbing I,

Pembimbing II,

Prof. Dr. Azharsyah, S.E., Ak., M.S.O.M.

Ismail Nura, ME.

NIP. 197811122005011003

NIP. 199506052025051004

AR - RANIRY

Mengetahui,

Ketua Program Studi Perbankan Syariah

Nei k

Dr. Nevi Hasnita, S.Ag., M.Ag

NIP.19771105200604200

PENGESAHAN SIDANG MUNAQASYAH SKRIPSI

**PENGARUH LITERASI DAN KEAMANAN DATA PRIBADI
TERHADAP KEWASPADAAN TERHADAP PENIPUAN DIGITAL
PADA NASABAH BANK ACEH SYARIAH DI KOTA BANDA
ACEH**

Rifqi Aldian
NIM: 220603092

Telah Disidangkan oleh Dewan Penguji Skripsi
Fakultas Ekonomi dan Bisnis Islam UIN Ar-Raniry Banda Aceh
dan Dinyatakan Lulus serta Diterima Sebagai Salah Satu Syarat untuk
Menyelesaikan Program Studi Strata Satu (S-1) dalam Bidang Perbankan
Syariah

Pada hari/tanggal: Rabu, 26 Agustus 2026 M
13 Rabiul Awal 1448 H
Banda Aceh
Dewan Penguji Sidang Skripsi

Ketua,

Sekretaris,

Prof. Dr. Azharsyah, S.E., Ak., M.S.O.M.

Ismail Nura, ME.

NIP. 197811122005011003

NIP. 199506052025051004

Penguji I,

Penguji II,

Fithriady, Lc., M.A., Ph.D

Dr. Evy Iskandar, S.E., M.Si., Ak., CPA

NIP. 198008122006041004

NIP. 198511222023211015

Mengetahui,

Dekan Fakultas Syari'ah dan Hukum
UIN Ar-Raniry Banda Aceh

Prof. Dr. Hafas Furgani, M.Ec

NIP. 198006252009011009



**KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI AR-RANIRY BANDA
ACEH**

UPT. PERPUSTAKAAN

Jl. Sheikh Abdur Rauf Kopelma Darussalam Banda Aceh
Telp. 0651-7552921, 7551857, Fax. 0651-7552922
Web: www.library.ar-raniry.ac.id, Email: fsh@ar-raniry.ac.id

**FROM PERNYATAAN PERSETUJUAN PUBLIKASI KARYA
ILMIAH MAHASISWA UNTUK KEPENTINGAN AKADEMIK**

Yang bertandatangan di bawah ini

Nama : Rifqi Aldian
NIM : 220603092
Program Studi : Perbankan Syariah
Fakultas : Ekonomi Dan Bisnis Islam

Demi mengembangkan ilmu pengetahuan, menyetujui untuk memberikan kepada UPT Perpustakaan Universitas Islam Negeri (UIN) Ar-Raniry Banda Aceh, Hak Bebas Royalti Non-Eksklusif (Non-Exclusive Royalty-Free Right) atas karya ilmiah:

☐ Tugas Akhir ☐ KKKU ☐ Skripsi

Yang berjudul: Pengaruh Literasi dan Keamanan Data Pribadi Terhadap Kewaspadaan Terhadap Penipuan Digital pada Nasabah Bank Aceh Syariah di Kota Banda Aceh

Beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Eksklusif ini, UPT Perpustakaan UIN Ar-Raniry Banda Aceh berhak menyimpan, mengalih media formatkan, mengelola, mendiseminasikan, dan mempublikasikannya di internet atau media lain.

Secara fulltext untuk kepentingan akademik tanpa perlu meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis, pencipta dan atau penerbit karya ilmiah tersebut. UPT Perpustakaan UIN Ar-Raniry Banda Aceh akan terbebas dari segala bentuk tuntutan hukum yang timbul atas pelanggaran hak cipta dalam karya ilmiah saya ini. Demikian pernyataan ini yang saya buat dengan sebenarnya.

Dibuat di **UIN** Banda Aceh

Pada tanggal : 26 Agustus 2026

Mengetahui,

Penulis

Rifqi Aldian

NIM: 220603092

Pembimbing I

Prof. Dr. Azharsyah, S.E., Ak., M.S.O.M.

NIP. 197811122005011003

Pembimbing II

Ismail Nura, M.E.

NIP. 199506052025051004

KATA PENGANTAR



Syukur Alhamdulillah kita panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat serta karunia-Nya sehingga penulis mampu menyelesaikan penyusunan skripsi yang berjudul “Pengaruh Literasi dan Keamanan Data Pribadi Terhadap Kewaspadaan Terhadap Penipuan Digital pada Nasabah Bank Aceh Syariah di Kota Banda Aceh.” Shalawat beriring salam tidak lupa kita curahkan kepada junjungan Nabi besar kita Nabi Muhammad SAW, yang telah mendidik seluruh umatnya untuk menjadi generasi terbaik di muka bumi ini.

Dalam penulisan skripsi ini, penulis menyadari bahwa ada beberapa kesilapan dan kesulitan, namun berkat bantuan dari berbagai pihak Alhamdulillah penulis dapat menyelesaikan tugas akhir ini. Oleh karena itu penulis menyampaikan ucapan terima kasih yang sedalam-dalamnya kepada:

1. Prof. Dr. Hafas Furqani, M.Ec selaku Dekan Fakultas Ekonomi dan Bisnis Islam UIN Ar-Raniry.
2. Dr. Nevi Hasnita, M.Ag dan Ana Fitria, M.Sc selaku Ketua dan Sekretaris Program Studi Perbankan Syariah Fakultas Ekonomi dan Bisnis Islam, UIN Ar- Raniry Banda Aceh.
3. Hafiizh Maulana, S.P., S.HI., M.E selaku Ketua Laboratorium Fakultas Ekonomi dan Bisnis Islam UIN Ar-Raniry Banda Aceh.

4. Prof. Dr. Azharsyah,S.E., M.S.O.M. dan Ismail Nura, M.E. selaku pembimbing I dan pembimbing II yang telah banyak meluangkan waktu dan pikiran dalam memberikan masukan-masukan dan arahan dalam menyelesaikan skripsi ini.
5. Prof. Dr. Azharsyah,S.E., M.S.O.M. selaku dosen Penasehat akademik yang telah membimbing serta memberikan nasehat dan motivasi terbaik untuk penulis selama menempuh pendidikan di program studi strata satu (S1) Perbankan Syariah. Seluruh dosen dan civitas akademika Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Ar-Raniry Banda Aceh.
6. Teristimewa kepada kedua orang tua , Ayah Safriman dan Ibu Emria Aida, penulis menyampaikan terima kasih yang sebesar-besarnya atas segala cinta, kasih sayang, doa, pengorbanan, perhatian, dukungan, serta motivasi yang senantiasa diberikan kepada penulis. Terima kasih telah menjadi tempat untuk pulang, sumber kekuatan, dan alasan bagi penulis untuk terus berjuang dalam menyelesaikan pendidikan. Setiap doa dan pengorbanan yang diberikan menjadi bagian yang tidak terpisahkan dari perjalanan penulis hingga dapat menyelesaikan pendidikan dan meraih gelar sarjana. Penulis juga menyampaikan terima kasih yang tulus kepada abang Zikra Mubarak, serta seluruh keluarga besar yang senantiasa memberikan doa, semangat,

perhatian, dukungan, dan kasih sayang kepada penulis. Terima kasih atas setiap bentuk kepedulian dan motivasi yang diberikan, baik dalam keadaan suka maupun duka, sehingga penulis dapat melewati berbagai proses dan tantangan selama menempuh pendidikan.

7. Penulis mengucapkan terima kasih yang sebesar-besarnya kepada sahabat seperjuangan, Rio Seftiawan, Muhammad Agnial Mahari, Muhammad Al' Adiyat, Andika Pratama, Kevin Fathuriansyah, Rizky Fajamaputra, yang telah menjadi rumah yang nyaman dan tempat pulang di perantauan, serta selalu hadir dalam setiap kebahagiaan maupun kesulitan. Nurul Fadhillah, Putri maulidya, Nazilatul Fitri, Ulfa Natasya, Wahyuni Sahara, Siti Yara Khalishah, yang telah menemani perjalanan perkuliahan penulis sejak semester pertama hingga penyelesaian skripsi.

Banda Aceh, 13 Agustus 2026

Penulis,

Rifqi Aldian

TRANSLITERASI ARAB-LATIN DAN SINGKATAN
Keputusan Bersama Menteri Agama dan Menteri P dan K
Nomor: 158 Tahun 1987– Nomor: 0543b/u1987

1. Konsonan

No.	Arab	Latin	No.	Arab	Latin
1	ا	Tidak dilambangkan	16	ط	Ṭ
2	ب	B	17	ظ	Ẓ
3	ت	T	18	ع	‘
4	ث	Ṣ	19	غ	G
5	ج	J	20	ف	F
6	ح	Ḥ	21	ق	Q
7	خ	Kh	22	ك	K
8	د	D	23	ل	L
9	ذ	Ẓ	24	م	M
10	ر	R	25	ن	N
11	ز	Z	26	و	W
12	س	S	27	ه	H
13	ش	Sy	28	ء	‘
14	ص	Ṣ	29	ي	Y
15	ض	Ḍ			

2. Vocal

Vokal Bahasa Arab, seperti vokal bahasa Indonesia, terdiri dari vokal tunggal atau monoftong dan vokal rangkap atau diftong.

a. Vocal Tunggal

Vokal tunggal bahasa Arab yang lambangnya berupa tanda atau harkat, transliterasinya sebagai berikut:

Tanda	Nama	Huruf Latin
َ	<i>Fathah</i>	A
ِ	<i>Kasrah</i>	I
ُ	<i>Dammah</i>	U

b. Vocal Rangkap

Vokal rangkap bahasa Arab yang lambangnya berupa gabungan antara harkat dan huruf, transliterasinya gabungan huruf, yaitu:

Tanda dan Huruf	Nama	Gabungan Huruf
َـيْ	<i>Fathah dan ya</i>	Ai
َـوْ	<i>Fathah dan wau</i>	Au

Contoh:

كَيْفَ : *Kaifa*

هَوْلَ : *Haula*

3. Maddah

Maddah atau vokal panjang yang lambangnya berupa harakat dan huruf, transliterasinya berupa huruf dan tanda, yaitu:

Harkat dan Huruf	Nama	Huruf dan Tanda
أَ / اِيْ	<i>Fathah dan alif atau ya</i>	Ā
إِ	<i>Kasrah dan ya</i>	Ī
ئِ	<i>Dammah dan wau</i>	Ū

Contoh:

قَالَ : *qāla*
رَمَى : *ramā*
قِيلَ : *qīla*
يَقُولُ : *yaqūlu*

4. Ta Marbutah (ة)

Transliterasi untuk ta marbutah ada dua.

- Ta marbutah (ة) hidup

Ta marbutah (ة) yang hidup atau mendapat harkat fathah, kasrah, dan dammah, transliterasinya adalah t.

- Ta marbutah (ة) mati

Ta marbutah (ة) yang mati atau mendapat harkat sukun, transliterasinya adalah h.

- c. Kalau pada suatu kata yang akhir katanya ta marbutah (ة) diikuti oleh kata yang menggunakan kata sandang al, serta bacaan kedua kata itu terpisah maka ta marbutah (ة) itu ditransliterasikan dengan h.

Contoh:

رَوْضَةُ الْأَطْفَالِ : *raudah al-atfāl/ raudatulatfāl*

الْمَدِينَةُ الْمُنَوَّرَةُ : *Al-Madīnah Al-Munawwarah*

طَلْحَة : *Talhah*

Catatan

Modifikasi

1. Nama orang berkebangsaan Indonesia ditulis seperti biasa tanpa transliterasi, seperti M. Syuhudi Ismail, sedangkan nama-nama lainnya ditulis sesuai kaidah penerjemahan. Contoh: Hamad Ibn Sulaiman.
2. Nama Negara dan kota ditulis menurut ejaan Bahasa Indonesia, seperti Mesir, bukan Misr; Beirut, bukan Bayrut; dan sebagainya.
3. Kata-kata yang sudah dipakai (serapan) dalam kamus Bahasa Indonesia tidak ditransliterasi. Contoh: Tasauf, bukan Tasawuf.

ABSTRAK

Nama Mahasiswa : Rifqi Aldian
Nim : 220603092
Fakultas : Ekonomi dan Bisnis Islam
Program Studi : Perbankan Syariah
Judul : Pengaruh Literasi dan Keamanan Data Pribadi Terhadap Kewaspadaan Terhadap Penipuan Digital pada Nasabah Bank Aceh Syariah di Kota Banda Aceh
Pembimbing 1 : Prof. Dr. Azharsyah, S.E., Ak., M.S.O.M.
Pembimbing 2 : Ismail Nura, M.E.

Literasi digital dan keamanan data pribadi merupakan aspek penting dalam meningkatkan kewaspadaan terhadap penipuan digital. Penelitian ini bertujuan menganalisis pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh. Penelitian ini menggunakan metode kuantitatif melalui penyebaran kuesioner yang disebarakan kepada 384 responden dengan menggunakan rumus cochrane. Penelitian ini menggunakan teknik sampling nonprobability sampling dengan model purposive sampling. Data dikumpulkan menggunakan kuesioner dan dianalisis dengan regresi linier berganda menggunakan SPSS 25. Hasil penelitian menunjukkan bahwa literasi digital dan keamanan data pribadi secara parsial maupun simultan berpengaruh positif dan signifikan terhadap kewaspadaan terhadap penipuan digital. Artinya, semakin baik literasi digital dan keamanan data pribadi, semakin tinggi kewaspadaan mereka terhadap penipuan digital. Kedua variabel menjelaskan 75,6% variasi kewaspadaan. Perbankan disarankan meningkatkan edukasi nasabah serta memperkuat keamanan melalui OTP dan verifikasi dua langkah.

Kata kunci: *Literasi Digital, Keamanan Data Pribadi, Kewaspadaan terhadap Penipuan Digital.*

DAFTAR ISI

KATA PENGANTAR	v
TRANSLITERASI ARAB-LATIN DAN SINGKATAN	viii
ABSTRAK.....	xii
DAFTAR ISI	xiii
DAFTAR TABEL	xvi
DAFTAR GAMBAR	xvii
DAFTAR LAMPIRAN	xviii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	11
1.3 Tujuan Penelitian	11
1.4 Manfaat Penelitian	12
1.5 Sistematika Penelitian.....	13
BAB II LANDASAN TEORI.....	15
2.1 Perbankan Digital	15
2.1.1 Pengertian Perbankan Digital.....	15
2.1.2 Layanan Perbankan Digital.....	16
2.1.3 Pengertian Nasabah Bank	17
2.1.4 Hak dan Kewajiban Nasabah dalam Transaksi Digital.....	18
2.1.5 Risiko Kejahatan Digital dalam Perbankan	20
2.2 Kewaspadaan Terhadap Penipuan Digital	21
2.2.1 Pengertian Kewaspadaan Terhadap Penipuan Digital	21
2.2.2 Protection Motivation Theory (PMT)	22
2.2.3 Penipuan dalam Perspektif Islam	23
2.2.4 Faktor-faktor yang Mempengaruhi Penipuan Digital	26
2.2.5 Jenis-jenis Penipuan Digital	28
2.2.6 Indikator Penipuan Digital	30
2.3 Literasi Digital	32
2.3.1 Pengertian Literasi Digital	32
2.3.2 Faktor-faktor yang Mempengaruhi Literasi Digital	32
2.3.3 Aspek-aspek Literasi Digital.....	33
2.3.4 Tingkatan Literasi Digital	35
2.3.5 Indikator Literasi Digital.....	36
2.4 Keamanan Data Pribadi	38
2.4.1 Pengertian Keamanan Data Pribadi	38

2.4.2 Jenis-jenis Data Pribadi.....	38
2.4.3 Prinsip Perlindungan Data Pribadi	39
2.4.4 Risiko Kebocoran Data Pribadi.....	42
2.4.5 Indikator Keamanan Data Pribadi.....	44
2.5 Penelitian Terdahulu.....	45
2.6 Hubungan Antar Variabel.....	58
2.6.1 Hubungan Literasi Digital terhadap Kewaspadaan terhadap Penipuan Digital	58
2.6.2 Hubungan Keamanan Data Pribadi terhadap Kewaspadaan terhadap Penipuan Digital.....	59
2.6.3 Hubungan Literasi Digital dan Keamanan Data Pribadi terhadap Kewaspadaan terhadap Penipuan Digital	60
2.7 Kerangka Berpikir.....	60
2.8 Hipotesis Penelitian	62
BAB III METODE PENELITIAN	63
3.1 Jenis Penelitian	63
3.2 Lokasi Dan Waktu Penelitian	63
3.3 Populasi dan Sampel.....	64
3.3.1 Populasi.....	64
3.3.2 Sampel.....	64
3.4 Sumber dan Teknik Pengumpulan Data	68
3.4.1 Sumber Data.....	68
3.4.2 Teknik Pengumpulan Data.....	68
3.5 Definisi dan Operasional Variabel.....	69
3.5.1 Variabel Dependen (Y).....	69
3.5.2 Variabel Independen (X).....	69
3.5.3 Operasional Variabel.....	71
3.6 Skala Pengukuran	73
3.7 Metode Analisis Data.....	74
3.7.1 Uji Keabsahan Data	74
3.7.2 Uji Asumsi Klasik.....	75
3.8 Uji Regresi Linear Berganda	77
3.9 Uji Hipotesis	78
3.9.1 Uji T (Uji Parsial)	78
3.9.2 Uji F (Uji Simultan)	79
3.9.3 Uji Koefisien Determinasi (R^2)	80
BAB IV HASIL PENELITIAN DAN PEMBAHASAN	81
4.1 Gambaran Umum Lokasi Penelitian.....	81

4.2 Hasil Penelitian	82
4.2.1 Karakteristik Responden	83
4.3 Tanggapan Responden Terhadap Variabel Penelitian	88
4.3.1 Tanggapan Responden Terhadap Variabel Literasi Digital (X1)	89
4.3.2 Tanggapan Responden Terhadap Variabel Keamanan Data Pribadi (X2)	91
4.3.3 Tanggapan Responden Terhadap Variabel Kewaspadaan terhadap Penipuan Digital (Y)	94
4.4 Hasil Uji Validitas dan Reliabilitas	96
4.4.1 Uji Validitas	96
4.4.2 Uji Reliabilitas	97
4.5 Hasil Uji Asumsi Klasik	98
4.5.1 Uji Normalitas	98
4.5.2 Uji Multikolinearitas	101
4.5.3 Uji Heteroskedastisitas	102
4.6 Hasil Uji Regresi Linear Berganda	103
4.7 Hasil Uji Hipotesis	104
4.7.1 Uji Parsial (Uji t)	104
4.7.2 Uji Simultan (Uji F)	105
4.7.3 Uji Determinasi (R^2)	106
4.8 Pembahasan	107
4.8.1 Pengaruh Literasi Digital terhadap Kewaspadaan terhadap Penipuan Digital	108
4.8.2 Pengaruh Keamanan Data Pribadi terhadap Kewaspadaan terhadap Penipuan Digital	110
4.8.3 Pengaruh Literasi Digital dan Keamanan Data Pribadi secara Simultan terhadap Kewaspadaan terhadap Penipuan Digital	113
BAB V	119
5.1 Kesimpulan	119
5.2 Saran	121
DAFTAR PUSTAKA	124
LAMPIRAN	1

DAFTAR TABEL

Tabel 4. 1 Luas Wilayah dan Jumlah Penduduk Masing-Masing Kecamatan di Kota Banda Aceh.....	82
Tabel 4. 2 Tanggapan Responden Terhadap Variabel Literasi Digital (X1).....	89
Tabel 4. 3 Tanggapan Responden Terhadap Variabel Keamanan Data Pribadi (X2)	92
Tabel 4. 4 Tanggapan Responden Terhadap Variabel Kewaspadaan terhadap Penipuan Digital (Y).....	94
Tabel 4. 5 Hasil Uji Validitas.....	96
Tabel 4. 6 Hasil Uji Reliabilitas.....	98
Tabel 4. 7 Hasil Uji Normalitas (One-Sample Kolmogorov-Smirnov Test).....	99
Tabel 4. 8 Hasil Uji Multikolinearitas	101
Tabel 4. 9 Hasil Uji Regresi Linear Berganda	103
Tabel 4. 10 Hasil Uji Simultan (Uji F)	106
Tabel 4. 11 Hasil Uji Determinasi (R^2).....	107



DAFTAR GAMBAR

Gambar 4. 1 Diagram Karakteristik Responden Berdasarkan Domisili	83
Gambar 4. 2 Diagram Karakteristik Responden Berdasarkan Jenis Kelamin	84
Gambar 4. 3 Diagram Karakteristik Responden Berdasarkan Usia	85
Gambar 4. 4 Diagram Karakteristik Responden Berdasarkan Pendidikan Terakhir.....	86
Gambar 4. 5 Diagram Karakteristik Responden Berdasarkan Pekerjaan	87
Gambar 4. 6 Diagram Karakteristik Responden Berdasarkan Pengalaman Menggunakan Layanan Digital Bank Aceh Syariah ..	88
Gambar 4. 7 Normal P-P Plot of Regression Standardized Residual	100
Gambar 4. 8 Hasil Uji Heteroskedastisitas (Scatterplot).....	102



DAFTAR LAMPIRAN

- Lampiran 1 Kuesioner Penelitian
- Lampiran 2 Hasil Tabulasi Kuesioner Responden
- Lampiran 3 Hasil Uji Statistik
- Lampiran 4 Hasil Uji Asumsi Klasik
- Lampiran 5 Hasil Uji Regresi Linear Berganda
- Lampiran 6 Hasil Uji Hipotesis
- Lampiran 7 Tabel R
- Lampiran 8 Daftar Riwayat Hidup



BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi di era digital telah membawa transformasi besar dalam berbagai aspek kehidupan manusia, termasuk dalam sektor keuangan dan layanan perbankan. Digitalisasi layanan finansial memungkinkan masyarakat melakukan transaksi secara cepat, praktis, dan efisien melalui berbagai platform digital. Namun, kemajuan tersebut juga menghadirkan tantangan baru berupa meningkatnya kejahatan siber, khususnya penipuan keuangan digital dan pencurian data pribadi. Permasalahan ini menjadi perhatian serius di Indonesia mengingat literasi digital masyarakat yang belum merata serta masih rendahnya pemahaman terhadap pentingnya keamanan data pribadi (Hapsari & Pambayun, 2023).

Aktivitas seperti penipuan digital, peretasan data, dan pencurian identitas terus mengalami peningkatan. Rendahnya kesadaran masyarakat terhadap pentingnya menjaga keamanan informasi pribadi sering kali dimanfaatkan oleh pelaku kejahatan siber untuk menjalankan aksinya (Siagian dkk., 2024). Peningkatan jumlah pengguna internet di berbagai sektor turut memperbesar potensi risiko kejahatan digital (Wahib dkk., 2022). Pesatnya perkembangan teknologi komunikasi mempercepat arus penyebaran informasi. Di satu sisi, teknologi dapat dimanfaatkan

sebagai sarana memperoleh berbagai sumber pengetahuan, namun di sisi lain kemudahan penyebaran informasi juga berpotensi menimbulkan penyalahgunaan, sehingga diperlukan keterampilan literasi digital atau literasi media dalam mengelola informasi secara bijak (Maharan dkk., 2021).

Satgas Pemberantasan Aktivitas Keuangan Ilegal (Satgas PASTI) di bawah koordinasi Otoritas Jasa Keuangan (OJK) menegaskan bahwa aktivitas keuangan ilegal dan penipuan digital terus berkembang dengan modus yang semakin kompleks, terutama melalui media sosial, aplikasi pesan instan, situs web, dan berbagai platform digital lainnya. Ancaman ini semakin meningkat dengan pemanfaatan teknologi *Artificial Intelligence* (AI). Dalam siaran pers 15 November 2025, Satgas PASTI mengungkapkan bahwa pelaku penipuan menggunakan teknologi voice cloning dan deepfake untuk meyakinkan korban agar menyerahkan uang maupun data pribadi (OJK, 2025).

Tabel 1. 1 Laporan Penipuan Digital di Indonesia Berdasarkan Data Indonesia Anti-Scam Centre (IASC) Tahun 2025

No	Indikator	Jumlah
1	Total Laporan Penipuan	343.402 laporan
2	Rekening Terindikasi Terlibat Penipuan	563.558 rekening
3	Rekening yang Berhasil Diblokir	106.222 rekening
4	Total Kerugian Korban	Rp7,8 triliun
5	Dana yang Berhasil Diamankan	Rp386,5 miliar

Sumber: Indonesia Anti-Scam Centre (IASC) – OJK (2025).

Indonesia Anti-Scam Centre (IASC) mencatat bahwa sejak 22 November 2024 hingga 11 November 2025 terdapat 343.402 laporan penipuan, dengan 563.558 rekening terindikasi terlibat penipuan dan 106.222 rekening berhasil diblokir. Total kerugian korban mencapai Rp7,8 triliun, sementara dana yang berhasil diamankan sebesar Rp386,5 miliar. Angka tersebut menunjukkan bahwa meskipun upaya penindakan terus diperkuat, tingkat kerugian masyarakat akibat penipuan digital masih sangat tinggi (OJK, 2025).

Tabel 1. 2 Statistik Pengalaman dan Jenis Penipuan Digital di Indonesia Berdasarkan Laporan GASA Tahun 2025

No	Indikator	Persentase
1	Orang dewasa mengalami penipuan (12 bulan terakhir)	35%
2	Responden merasa percaya diri mengenali penipuan	86%
3	Responden mengalami penipuan hingga 3 kali setahun	12%
4	Responden mengalami penipuan >11 kali setahun	4%
5	Penipuan investasi	63%
6	Penipuan belanja online	62%
7	Penipuan hadiah palsu	55%

Sumber: GASA (2025)

Laporan GASA (2025), menyebutkan bahwa 35% orang dewasa di Indonesia mengalami penipuan digital dalam 12 bulan terakhir. Sebanyak 86% responden merasa percaya diri dapat

mengenali modus penipuan, namun pada kenyataannya banyak yang tetap menjadi korban. Bahkan, 12% responden mengalami penipuan hingga tiga kali dalam setahun, dan 4% lainnya mengalami lebih dari sebelas kali. Jenis penipuan yang paling dominan meliputi penipuan investasi (63%), penipuan belanja online (62%), dan penipuan hadiah palsu (55%). Temuan ini menunjukkan adanya kesenjangan antara kepercayaan diri masyarakat dalam mengenali penipuan dan kemampuan nyata mereka dalam menghindarinya.

Data tersebut menunjukkan bahwa penipuan digital merupakan fenomena yang terjadi dalam berbagai aktivitas digital dan tidak hanya terbatas pada sektor perbankan, seperti investasi, belanja online, media sosial, hadiah palsu, dan layanan keuangan digital.

Meskipun demikian, sektor perbankan tetap penting untuk diperhatikan karena berkaitan langsung dengan penyimpanan dan pengelolaan dana masyarakat. Berbeda dengan beberapa bentuk penipuan digital lainnya, penipuan pada layanan perbankan dapat menimbulkan kerugian finansial yang secara langsung terlihat melalui berkurangnya atau berpindahnya dana dari rekening nasabah. Risiko tersebut semakin besar apabila pelaku memperoleh informasi penting, seperti PIN, password, kode OTP, atau data pribadi nasabah.

Dengan demikian, data GASA dan IASC digunakan untuk menunjukkan bahwa penipuan digital merupakan fenomena yang

luas dan terjadi dalam berbagai aktivitas masyarakat. Sementara itu, pemilihan konteks perbankan dalam penelitian ini didasarkan pada karakteristik layanan perbankan yang berkaitan langsung dengan dana nasabah serta risiko penyalahgunaan data dan akses akun yang dapat menimbulkan kerugian finansial secara langsung. Oleh karena itu, kewaspadaan nasabah terhadap berbagai modus penipuan digital menjadi penting untuk diteliti.

Data tersebut menunjukkan bahwa penipuan digital merupakan fenomena yang terjadi dalam berbagai aktivitas digital dan tidak hanya terbatas pada sektor perbankan, seperti investasi, belanja online, media sosial, hadiah palsu, dan layanan keuangan digital. Meskipun demikian, sektor perbankan penting untuk diperhatikan karena berkaitan langsung dengan penyimpanan dan pengelolaan dana masyarakat. Berbeda dengan beberapa bentuk penipuan digital lainnya, penipuan pada layanan perbankan dapat menimbulkan kerugian finansial yang secara langsung terlihat melalui berkurangnya atau berpindahnya dana dari rekening nasabah.

Kewaspadaan terhadap penipuan digital menjadi hal yang penting seiring dengan meningkatnya penggunaan layanan perbankan berbasis digital. Kewaspadaan dapat dilihat dari kesadaran dan perhatian pengguna terhadap kemungkinan terjadinya penipuan melalui media digital, termasuk kemampuan dalam mengenali informasi, komunikasi, atau permintaan yang mencurigakan. Dalam penggunaan layanan perbankan online,

phishing awareness berkaitan dengan pengetahuan pengguna mengenai *phishing* serta kesadaran terhadap risiko keamanan yang dapat muncul ketika menggunakan layanan (Nur'aini & Simanjuntak, 2025).

Salah satu bentuk penipuan digital yang marak terjadi di masyarakat adalah penipuan melalui tautan *phishing* yang disebarkan melalui email maupun media sosial seperti WhatsApp, Telegram, Facebook, dan berbagai platform digital lainnya. Modus ini bertujuan untuk memperoleh data pribadi korban secara ilegal yang kemudian dimanfaatkan untuk kepentingan finansial pelaku (Sahfitri & Rosmalinda, 2024).

Penggunaan QRIS, *mobile banking*, dan *e-wallet* memang memberikan efisiensi transaksi, tetapi juga menciptakan ruang baru bagi munculnya berbagai modus kejahatan siber. Penelitian Syahrin dkk (2025) di Aceh menunjukkan bahwa keamanan belum menjadi pertimbangan utama masyarakat dalam melakukan transaksi digital. Pengguna lebih tertarik pada kemudahan dan kecepatan, sementara aspek keamanan sering diabaikan. Pengabaian aspek ini meningkatkan risiko pembobolan akun, transaksi fiktif, serta pencurian data pribadi.

Polresta Banda Aceh mencatat berbagai modus penipuan seperti jual beli fiktif, undian berhadiah, serta penipuan yang mengatasnamakan pejabat daerah dengan kerugian hingga ratusan juta rupiah (Serambinews.com, 2025). Kasus lain yang diberitakan oleh AnalisaAceh.com (2025) menunjukkan seorang warga Pidie

mengalami kerugian Rp35 juta akibat akun media sosial palsu yang mencatut nama Ketua PWI Aceh, lengkap dengan foto profil dan penggunaan bahasa daerah untuk membangun kepercayaan korban. Selain itu, maraknya penipuan digital yang mengatasnamakan PT Bank Aceh Syariah dengan berbagai modus *phishing* menunjukkan bahwa keamanan data pribadi seperti PIN, password, dan kode OTP harus dijaga dengan baik karena permintaan data tersebut dengan mengatasnamakan bank dapat dipastikan merupakan bentuk penipuan (Modusaceh.co, 2025).

Berbagai penelitian menegaskan bahwa rendahnya literasi digital dan kesadaran keamanan data pribadi menjadi faktor utama meningkatnya risiko penipuan digital. Penelitian Nisa dkk (2025) menemukan bahwa kurangnya pemahaman individu terhadap konsep keamanan digital, seperti penggunaan kata sandi kuat, autentikasi dua faktor, serta kemampuan mengenali *phishing*, menyebabkan tingginya kerentanan terhadap kejahatan siber. Hasil kegiatan edukasi menunjukkan peningkatan pemahaman peserta hingga 57%, yang menandakan bahwa literasi digital efektif dalam memperkuat kesadaran perlindungan data pribadi.

Penelitian Napitupulu & Susanti (2025) juga menegaskan bahwa literasi digital merupakan faktor penting dalam mencegah penipuan online, khususnya pada kelompok rentan. Literasi digital tidak hanya mencakup kemampuan teknis menggunakan perangkat digital, tetapi juga keterampilan analitis dalam mengevaluasi

informasi secara kritis, memisahkan fakta dari opini, serta memahami risiko di ruang digital (Naufal, 2021).

Penelitian Ribeiro dkk (2024) menemukan bahwa *technology competencies* tidak berpengaruh signifikan terhadap kerentanan phishing. Koefisien negatif menunjukkan adanya kecenderungan bahwa peningkatan kompetensi teknologi diikuti oleh penurunan kerentanan terhadap phishing. Namun, hubungan tersebut tidak signifikan secara statistik karena kompetensi teknologi bukan merupakan faktor yang secara mandiri cukup kuat dalam memprediksi kerentanan phishing setelah variabel lain diperhitungkan. Hal ini menunjukkan bahwa kemampuan menggunakan teknologi saja belum tentu cukup untuk melindungi individu dari phishing, kemampuan yang lebih spesifik, seperti kemampuan mendeteksi dan membedakan pesan phishing dari pesan yang sah, dapat memiliki peran yang lebih menentukan.

Selain faktor literasi digital, aspek keamanan pada platform digital juga perlu menjadi perhatian. Kelemahan sistem keamanan memungkinkan pelaku mengakses basis data pengguna atau meniru identitas resmi untuk menipu korban. Oleh karena itu, diperlukan upaya berkelanjutan dalam memperkuat sistem keamanan serta meningkatkan edukasi kepada pengguna mengenai cara mengidentifikasi potensi penipuan, memverifikasi keaslian informasi, dan tidak membagikan data pribadi secara sembarangan (Gunawan dkk., 2024). Upaya preventif dan represif melalui

peningkatan kesadaran serta perlindungan hukum juga diperlukan guna menekan angka penipuan digital (Bodhi & Tan, 2022).

Meskipun berbagai penelitian telah menunjukkan bahwa literasi digital dan keamanan data pribadi berperan dalam mencegah penipuan digital, hasil penelitian belum sepenuhnya konsisten. Ribeiro dkk. (2024) menemukan bahwa *technology competencies* tidak berpengaruh signifikan terhadap kerentanan *phishing*, sedangkan penelitian lain menunjukkan bahwa literasi digital mampu menurunkan risiko penipuan digital. Selain itu, sebagian besar penelitian terdahulu dilakukan pada masyarakat umum, pelajar, atau pengguna layanan digital dengan fokus pada pencegahan penipuan. Penelitian yang menguji pengaruh literasi digital dan keamanan data pribadi terhadap tingkat kerentanan penipuan pada nasabah perbankan, khususnya Bank Aceh Syariah di Kota Banda Aceh, masih sangat terbatas. Oleh karena itu, penelitian ini perlu dilakukan untuk memberikan bukti empiris pada konteks perbankan daerah.

Berdasarkan fenomena dan hasil penelitian terdahulu bahwa digitalisasi layanan perbankan telah memberikan kemudahan bagi masyarakat, namun di sisi lain turut meningkatkan risiko terjadinya penipuan keuangan digital. Tingginya kasus penipuan, besarnya kerugian korban, rendahnya tingkat literasi digital, serta lemahnya kesadaran masyarakat dalam menjaga keamanan data pribadi menjadi faktor utama yang meningkatkan kerentanan nasabah terhadap kejahatan siber. Berdasarkan latar belakang penelitian

tersebut peneliti tertarik untuk melakukan penelitian dengan judul **“Pengaruh Literasi Dan Keamanan Data Pribadi Terhadap Kewaspadaan Terhadap Penipuan Digital Pada Nasabah Bank Aceh Syariah Di Kota Banda Aceh”**.



1.2 Rumusan Masalah

Adapun rumusan masalah dalam penelitian ini yaitu:

1. Apakah Literasi Digital berpengaruh terhadap Kewaspadaan terhadap Penipuan Digital pada Nasabah Bank Aceh Syariah di Kota Banda Aceh?
2. Apakah Keamanan Data Pribadi berpengaruh terhadap Kewaspadaan terhadap Penipuan Digital pada Nasabah Bank Aceh Syariah di Kota Banda Aceh?
3. Apakah Literasi Digital dan Keamanan Data Pribadi berpengaruh secara simultan terhadap Kewaspadaan terhadap Penipuan Digital pada Nasabah Bank Aceh Syariah di Kota Banda Aceh?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini yaitu:

1. Untuk menganalisis pengaruh Literasi Digital terhadap Kewaspadaan terhadap Penipuan Digital pada Nasabah Bank Aceh Syariah di Kota Banda Aceh.
2. Untuk menganalisis pengaruh Keamanan Data Pribadi terhadap Kewaspadaan terhadap Penipuan Digital pada Nasabah Bank Aceh Syariah di Kota Banda Aceh.
3. Untuk menganalisis pengaruh Literasi Digital dan Keamanan Data Pribadi secara simultan terhadap Kewaspadaan terhadap Penipuan Digital pada Nasabah Bank Aceh Syariah di Kota Banda Aceh.

1.4 Manfaat Penelitian

Adapun manfaat penelitian ini dibagi menjadi tiga kategori, yaitu:

1. Manfaat Teoritis

Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan kajian akademik di bidang literasi digital dan keamanan data pribadi, khususnya yang berkaitan dengan kewaspadaan terhadap penipuan digital di sektor perbankan. Selain itu, penelitian ini dapat menjadi referensi bagi penelitian selanjutnya yang membahas perilaku nasabah dalam menghadapi risiko kejahatan digital.

2. Manfaat Praktis

Hasil penelitian ini diharapkan dapat memberikan informasi dan pemahaman kepada nasabah Bank Aceh Syariah di Kota Banda Aceh mengenai pentingnya literasi digital dan keamanan data pribadi dalam meningkatkan kewaspadaan terhadap penipuan digital. Dengan demikian, nasabah diharapkan dapat lebih waspada dalam mengenali berbagai bentuk dan modus penipuan digital serta lebih berhati-hati dalam melakukan transaksi dan menjaga keamanan data pribadi.

3. Manfaat Kebijakan

Penelitian ini diharapkan dapat menjadi bahan pertimbangan bagi pihak Bank Aceh Syariah serta lembaga

terkait dalam merancang program edukasi mengenai literasi digital dan keamanan data pribadi bagi nasabah, sehingga dapat meningkatkan kewaspadaan nasabah terhadap berbagai bentuk dan modus penipuan digital di sektor perbankan.

1.5 Sistematika Penelitian

Adapun sistematika penulisan dalam penelitian ini disusun sebagai berikut:

BAB I : Pendahuluan

Bab ini menguraikan latar belakang masalah yang berkaitan dengan meningkatnya risiko penipuan digital dalam layanan perbankan, khususnya pada nasabah Bank Aceh Syariah di Kota Banda Aceh. Selain itu, dibahas juga rumusan masalah, tujuan penelitian, serta manfaat penelitian baik secara teoritis, praktis, maupun kebijakan. Fokus utama penelitian ini adalah menganalisis pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan nasabah terhadap penipuan digital. Bab ini memberikan gambaran umum mengenai urgensi penelitian serta arah penelitian yang akan dilakukan.

BAB II : Landasan Teori

Bab ini menyajikan kajian teoritis yang relevan dengan penelitian, meliputi konsep literasi digital, keamanan data pribadi, dan kewaspadaan terhadap penipuan digital beserta indikator-indikatornya. Selain itu, dibahas pula teori-teori pendukung, penelitian terdahulu yang relevan, kerangka pemikiran, serta

pengembangan hipotesis yang akan diuji dalam penelitian ini. Bab ini berfungsi sebagai dasar konseptual dalam menganalisis hubungan antarvariabel.

BAB III : Metodologi Penelitian

Bab ini menjelaskan metode penelitian yang digunakan, yaitu pendekatan kuantitatif. Uraian dalam bab ini mencakup jenis dan sumber data, teknik pengumpulan data melalui kuesioner, populasi dan sampel penelitian, yaitu nasabah Bank Aceh Syariah di Kota Banda Aceh. Selain itu, dijelaskan juga definisi operasional variabel Literasi Digital, Keamanan Data Pribadi, dan Kewaspadaan terhadap Penipuan Digital, skala pengukuran, serta prosedur pengujian validitas dan reliabilitas instrumen penelitian.

BAB IV : Hasil Penelitian Dan Pembahasan

Pada bab ini, penulis menjelaskan dan memberikan penafsiran terhadap hasil dari pengolahan data serta memberi jawaban atas rumusan masalah.

BAB V : Penutup

Bab ini berisi kesimpulan yang diperoleh berdasarkan hasil penelitian dan rumusan masalah yang telah ditetapkan. Selain itu, disampaikan saran yang ditujukan kepada nasabah, pihak perbankan, khususnya Bank Aceh Syariah, serta pembuat kebijakan dalam meningkatkan literasi digital, keamanan data pribadi, dan kewaspadaan nasabah terhadap penipuan digital. Rekomendasi untuk penelitian selanjutnya juga disertakan sebagai bentuk kontribusi akademik.

BAB II

LANDASAN TEORI

2.1 Perbankan Digital

2.1.1 Pengertian Perbankan Digital

Penggunaan teknologi khususnya digital banking merupakan salah satu inovasi dari layanan yang bertujuan untuk memenuhi kebutuhan nasabah agar merasakan manfaatnya dan mudah dimengerti secara langsung hal ini berhubungan dengan penggunaan layanan dan perspektif nasabah pada layanan digital banking. Perbankan digital diharapkan dapat memberikan kemudahan, kemudahan dan keamanan dalam melakukan layanan perbankan dari kenyamanan rumah Anda, kapan saja, dari komputer atau laptop pribadi Anda dan menggunakan aplikasi seluler bank di ponsel cerdas atau tablet Anda. Ini meningkatkan kecepatan menyelesaikan tugas. Perbankan digital adalah komputerisasi perbankan tradisional jasa. Ini memungkinkan nasabah bank untuk mengakses perbankan produk dan menggunakan layanan perbankan melalui online/elektronik platform. Ini adalah digitalisasi dari semua operasi perbankan untuk menggantikan kehadiran fisik bank, menghilangkan kebutuhan nasabah dengan cara mengunjungi cabang (Reihandho & Fajarwati, 2020).

2.1.2 Layanan Perbankan Digital

Layanan perbankan digital ialah layanan perbankan elektronik dengan memaksimalkan pemanfaatan informasi yang dipunyai nasabah dalam rangka melayani nasabah secara lebih kilat lebih gampang serta sesuai dengan kebutuhan nasabah (Rahmah & Fasa, 2024). Perkembangan teknologi digital mendorong perbankan untuk beradaptasi dari sistem konvensional menuju sistem berbasis digital guna meningkatkan kualitas layanan dan daya saing industri keuangan. Layanan perbankan digital mencakup penggunaan media elektronik dalam penyediaan produk dan jasa keuangan, sehingga nasabah dapat melakukan transaksi secara mandiri tanpa harus datang ke kantor bank. Layanan ini diharapkan mampu memberikan pengalaman yang lebih cepat, mudah, serta sesuai dengan kebutuhan nasabah, sekaligus tetap memperhatikan aspek keamanan dalam setiap transaksi (Megawati & Kertiriasih, 2024).

Transformasi digital dalam sektor perbankan juga didorong oleh perkembangan *financial technology* (*fintech*) yang memperluas akses layanan keuangan serta meningkatkan efisiensi operasional. Adopsi teknologi digital memungkinkan perbankan menghadirkan inovasi layanan seperti *mobile banking*, pembayaran digital, serta berbagai platform berbasis aplikasi yang memudahkan interaksi antara bank dan nasabah (Rahmah & Fasa, 2024). Layanan perbankan digital mencakup berbagai bentuk layanan elektronik (*e-banking*) seperti anjungan tunai mandiri (ATM), *electronic data capture* (EDC), *internet banking*, *SMS banking*,

mobile banking, phone banking, hingga video banking. Kehadiran layanan ini memungkinkan nasabah untuk melakukan transaksi keuangan secara cepat, efektif, dan fleksibel tanpa terbatas oleh ruang dan waktu (Gisatriadi, 2024).

Digitalisasi perbankan tidak hanya meningkatkan efisiensi layanan, tetapi juga memperluas inklusi keuangan dengan menjangkau masyarakat yang sebelumnya sulit mengakses layanan perbankan. Namun demikian, implementasi layanan perbankan digital juga menghadapi berbagai tantangan, seperti aspek keamanan data, regulasi, serta kebutuhan edukasi nasabah agar dapat menggunakan layanan digital secara optimal dan aman (Gisatriadi, 2024).

2.1.3 Pengertian Nasabah Bank

Nasabah bank merupakan individu atau badan usaha yang memanfaatkan layanan perbankan untuk melakukan transaksi keuangan maupun penyimpanan dana. Dalam sistem perbankan, nasabah berperan sebagai pihak yang berinteraksi langsung dengan bank, baik sebagai penyimpan dana maupun pengguna berbagai produk dan jasa keuangan (Maulidiyah dkk., 2024). Secara konseptual, nasabah juga dapat dipahami sebagai pihak yang memiliki hubungan kontraktual dengan bank melalui pemanfaatan layanan seperti tabungan, pembiayaan, dan fasilitas transaksi lainnya, yang mencerminkan adanya keterikatan dalam aktivitas ekonomi yang saling menguntungkan (Ari dkk., 2024).

Nasabah tidak semata sebagai pengguna layanan, melainkan juga sebagai mitra dalam kegiatan usaha yang berlandaskan prinsip-prinsip syariah. Relasi antara bank dan nasabah dibangun melalui akad sesuai ketentuan Islam, seperti mudharabah, musyarakah, dan murabahah, sehingga menciptakan hubungan yang lebih partisipatif dan berkeadilan (Rozi & Samingan, 2024).

Keberadaan nasabah memiliki peran strategis dalam menentukan keberlangsungan operasional bank. Tingkat kepercayaan, kepuasan, dan loyalitas menjadi faktor utama dalam menjaga stabilitas serta pertumbuhan industri perbankan, khususnya di tengah persaingan dengan lembaga keuangan berbasis digital (Hartono & Keni, 2025). Nasabah bank tidak hanya dipahami sebagai pengguna layanan, tetapi juga sebagai elemen penting yang mendukung keberlanjutan dan perkembangan industri perbankan melalui interaksi, kepercayaan, serta partisipasi dalam berbagai produk dan layanan yang disediakan.

2.1.4 Hak dan Kewajiban Nasabah dalam Transaksi Digital

Nasabah memiliki sejumlah hak yang dijamin oleh peraturan perundang-undangan, khususnya terkait perlindungan data pribadi dan keamanan transaksi. Salah satu hak utama adalah perlindungan atas privasi, di mana setiap penggunaan data harus didasarkan pada persetujuan pemilik sebagaimana diatur dalam regulasi perlindungan data pribadi serta Undang-Undang Informasi dan Transaksi Elektronik (ITE). Ketentuan ini menegaskan adanya

kendali individu terhadap data pribadinya dalam aktivitas digital (Prasetyo, 2024). Nasabah berhak memperoleh informasi yang jelas, transparan, dan akurat mengenai layanan perbankan digital, termasuk risiko yang mungkin timbul (Sianturi dkk., 2024).

Perlindungan mencakup potensi kerugian akibat kesalahan sistem maupun penyalahgunaan data oleh pihak yang tidak bertanggung jawab. Regulasi perbankan dan perlindungan konsumen memberikan jaminan atas hak untuk mengajukan pengaduan serta memperoleh penyelesaian sengketa secara adil apabila terjadi pelanggaran dalam transaksi digital. Hal ini diperkuat oleh Undang-Undang Perlindungan Data Pribadi yang menempatkan individu sebagai subjek data dengan hak untuk mengetahui, mengakses, serta mengendalikan penggunaan datanya (Ferdiansyah dkk., 2025).

Terdapat kewajiban nasabah yang harus dipenuhi dalam penggunaan layanan digital. Salah satunya adalah menjaga kerahasiaan data pribadi dan kredensial akses, seperti PIN, password, dan kode OTP, agar tidak disalahgunakan. Kelalaian dalam hal ini dapat meningkatkan risiko penipuan digital. Faktor manusia seringkali menjadi penyebab utama kebocoran data, di mana karyawan yang kurang terlatih atau lalai dalam menjalankan protokol keamanan dapat menjadi titik kerentanan dalam sistem (Antoine dkk., 2025).

Pemahaman nasabah terhadap prosedur serta ketentuan penggunaan layanan perbankan digital, dan kepatuhan terhadap

aturan yang ditetapkan oleh pihak bank. Kepatuhan ini berperan penting dalam meminimalkan kesalahan transaksi maupun potensi penyalahgunaan layanan. Selain itu, peningkatan literasi digital menjadi hal yang esensial, terutama dalam memahami ancaman keamanan siber dan upaya pencegahannya. Hal ini sejalan dengan perkembangan teknologi perbankan yang menempatkan pengguna sebagai pihak yang turut bertanggung jawab dalam menjaga keamanan transaksi (Maharani & Purwanto, 2025). Keseimbangan antara hak dan kewajiban menjadi faktor krusial dalam menciptakan sistem transaksi digital yang aman dan terpercaya.

2.1.5 Risiko Kejahatan Digital dalam Perbankan

Perkembangan teknologi digital dalam sektor perbankan memberikan kemudahan dalam transaksi keuangan, namun di sisi lain turut meningkatkan potensi kejahatan digital yang merugikan nasabah. Transformasi layanan berbasis digital, seperti *mobile banking* dan *internet banking*, membuka peluang bagi pelaku kejahatan siber untuk memanfaatkan celah keamanan sistem maupun kelemahan pengguna (Rismawati dkk., 2024). Ancaman tersebut mencakup berbagai bentuk serangan, antara lain *phishing*, *malware*, *hacking*, dan *social engineering*. *Phishing* menjadi salah satu modus yang paling umum, di mana pelaku menyamar sebagai pihak bank melalui media komunikasi digital untuk memperoleh data sensitif nasabah seperti username, password, PIN, dan kode OTP. Selain itu, malware digunakan untuk menginfeksi perangkat

pengguna sehingga memungkinkan akses tidak sah terhadap data pribadi maupun sistem perbankan (Ananda dkk., 2024).

Kejahatan digital kerap melibatkan pencurian data pribadi (*data breach*) yang dimanfaatkan untuk transaksi ilegal atau pembobolan rekening. Praktik ini menjadi ancaman serius karena berpotensi menimbulkan kerugian finansial secara langsung sekaligus mengganggu keamanan sistem perbankan secara menyeluruh (Balaka dkk., 2023). Kompleksitas kejahatan ini juga meningkat seiring dengan penggunaan teknik manipulasi psikologis dalam *social engineering* untuk memperdaya korban (Hasanudin, 2025).

Tingkat literasi digital dan kesadaran terhadap keamanan data pribadi turut memengaruhi kerentanan nasabah. Minimnya pemahaman mengenai perlindungan informasi, seperti penggunaan kata sandi yang lemah atau kebiasaan membagikan data pribadi, dapat memperbesar risiko terjadinya serangan siber (Isnaini dkk., 2024). Risiko kejahatan digital dalam perbankan merupakan konsekuensi dari perkembangan teknologi yang tidak diimbangi dengan sistem keamanan yang kuat dan literasi digital yang memadai.

2.2 Kewaspadaan Terhadap Penipuan Digital

2.2.1 Pengertian Kewaspadaan Terhadap Penipuan Digital

Kewaspadaan terhadap penipuan digital merupakan kesadaran individu terhadap adanya risiko penipuan yang

dilakukan melalui media digital. Kewaspadaan tersebut dapat terlihat dari perhatian seseorang terhadap informasi, pesan, tautan, maupun permintaan data yang diterima melalui media digital. Dalam konteks perbankan online, kewaspadaan terhadap phishing berkaitan dengan pengetahuan pengguna mengenai phishing dan kemampuan untuk mengenali ancaman yang dapat membahayakan keamanan informasi pribadi maupun perbankan (Nur'aini & Simanjuntak, 2025).

2.2.2 Protection Motivation Theory (PMT)

Penelitian ini menggunakan *Protection Motivation Theory* sebagai *grand theory* untuk menjelaskan hubungan antara literasi digital, keamanan data pribadi, dan kewaspadaan terhadap penipuan digital. Teori ini pertama kali dikembangkan oleh Ronald W Rogers pada tahun 1975. *Protection Motivation Theory* menjelaskan bahwa individu akan terdorong melakukan tindakan perlindungan apabila mereka mampu memahami ancaman yang dihadapi dan memiliki kemampuan untuk mengurangi ancaman tersebut. Dalam konteks digital, ancaman tersebut berupa *phishing*, *social engineering*, pencurian data pribadi, dan berbagai bentuk penipuan digital lainnya (Winarto & Bisma, 2021).

Menurut Rogers dalam penelitian Winarto & Bisma (2021) proses perlindungan diri terbentuk melalui dua komponen utama yaitu *threat appraisal* dan *coping appraisal*. *Threat appraisal* berkaitan dengan penilaian individu terhadap tingkat ancaman yang dihadapi, sedangkan *coping appraisal* berkaitan dengan keyakinan

individu terhadap kemampuan dirinya dalam melakukan tindakan perlindungan. Dalam penelitian ini, literasi digital dipandang sebagai kemampuan individu dalam memahami informasi digital dan mengenali ancaman siber. Selanjutnya, keamanan data pribadi merupakan bentuk tindakan perlindungan yang dilakukan individu untuk menjaga kerahasiaan dan keamanan informasi pribadi. Kedua faktor tersebut diperkirakan berpengaruh terhadap penurunan risiko penipuan digital.

Teori ini relevan digunakan karena mampu menjelaskan bagaimana individu membangun perilaku perlindungan ketika menghadapi ancaman digital. Individu dengan tingkat literasi digital yang tinggi cenderung memiliki kemampuan lebih baik dalam mengevaluasi informasi, mengenali *phishing*, serta menjaga keamanan data pribadi. Sebaliknya, rendahnya kemampuan digital menyebabkan individu lebih rentan menjadi korban penipuan digital. Oleh karena itu, *Protection Motivation Theory* menjadi dasar yang kuat untuk menjelaskan hubungan antar variabel dalam penelitian ini.

2.2.3 Penipuan dalam Perspektif Islam

Penipuan dalam perspektif Islam berkaitan dengan tindakan kecurangan, tipu daya, atau penyamaran yang dapat merugikan pihak lain. Konsep penipuan antara lain dapat dijelaskan melalui istilah *ghisy* dan *tadllīs*, tetapi keduanya memiliki penekanan yang berbeda. *Ghisy* lebih merujuk pada tindakan kecurangan atau memberikan sesuatu yang tidak sesuai dengan keadaan sebenarnya,

sedangkan *tadlīs* lebih menekankan pada penyembunyian atau penyamaran informasi sehingga pihak lain memperoleh gambaran yang keliru. Dalam konteks digital, *ghisy* dapat berupa pemberian informasi atau tawaran palsu, sedangkan *tadlīs* dapat berupa penyamaran identitas, situs, akun, atau tautan yang dibuat menyerupai pihak resmi. Kedua bentuk tersebut dapat ditemukan dalam berbagai modus penipuan digital melalui media sosial, aplikasi pesan instan, maupun layanan perbankan digital. Oleh karena itu, pemahaman terhadap konsep *ghisy* dan *tadlīs* penting sebagai dasar untuk mengenali tindakan penipuan serta mendorong penerapan kejujuran dan amanah dalam aktivitas ekonomi dan transaksi digital (Wahyuni dkk., 2025)..

Islam melarang tindakan penipuan sebagaimana dijelaskan dalam Al-Qur'an Surah Al-Baqarah ayat 188 yang :

وَلَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْنُوا بِهَا إِلَى الْحُكَّامِ لِتَأْكُلُوا فَرِيقًا مِّنْ أَمْوَالِ النَّاسِ بِالْإِثْمِ وَأَنتُمْ تَعْلَمُونَ

Artinya: “Janganlah kamu makan harta di antara kamu dengan jalan yang batil dan (janganlah) kamu membawa (urusan) harta itu kepada para hakim dengan maksud agar kamu dapat memakan sebagian harta orang lain itu dengan jalan dosa, padahal kamu mengetahui”

Ayat tersebut menunjukkan bahwa penipuan merupakan bentuk pengkhianatan terhadap amanah yang telah dipercayakan kepada seseorang. Dalam praktik penipuan digital, pelaku biasanya menggunakan identitas palsu, manipulasi informasi, maupun

rekayasa komunikasi untuk memperoleh keuntungan tertentu. Tindakan tersebut mencerminkan perilaku tidak amanah dan bertentangan dengan nilai moral Islam yang menuntut setiap individu berlaku jujur serta bertanggung jawab dalam setiap transaksi dan interaksi sosial (Eriyan dkk., 2026).

Dalam Surah Al-Anfal ayat 27 Allah SWT juga melarang umat Islam untuk berkhianat terhadap amanah yang telah dipercayakan kepadanya. Arti Q.S Al-anfal Ayat 27 :

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَخُونُوا اللَّهَ وَالرَّسُولَ وَتَخُونُوا أَمَانَاتِكُمْ وَأَنْتُمْ تَعْلَمُونَ

Artinya: *“Wahai orang-orang yang beriman, janganlah kamu mengkhianati Allah dan Rasul serta janganlah kamu mengkhianati amanat yang dipercayakan kepadamu, sedangkan kamu mengetahui”*

Ayat tersebut menunjukkan bahwa penipuan merupakan bentuk pengkhianatan terhadap amanah yang telah dipercayakan kepada seseorang. Dalam praktik penipuan digital, pelaku biasanya menggunakan identitas palsu, manipulasi informasi, maupun rekayasa komunikasi untuk memperoleh keuntungan tertentu. Tindakan tersebut mencerminkan perilaku tidak amanah dan bertentangan dengan nilai moral Islam yang menuntut setiap individu berlaku jujur serta bertanggung jawab dalam setiap transaksi dan interaksi sosial. Dalam konteks penipuan digital, tindakan seperti *phishing*, *scam*, manipulasi data pribadi, hingga penipuan transaksi online termasuk kategori perbuatan batil karena

dilakukan dengan cara menyesatkan korban demi memperoleh keuntungan pribadi secara tidak sah (Eriyan dkk., 2026).

Dalam hukum pidana Islam (*fiqh jinayah*), penipuan dikategorikan sebagai *jarimah ta'zir*, yaitu tindak pidana yang jenis dan sanksinya tidak ditentukan secara langsung dalam Al-Qur'an maupun hadis, tetapi diserahkan kepada kebijakan hakim atau pemerintah berdasarkan tingkat kemudharatan yang ditimbulkan. Penetapan hukuman *ta'zir* bertujuan memberikan efek jera kepada pelaku sekaligus menjaga kemaslahatan masyarakat. Penipuan digital dipandang sebagai perbuatan yang mengancam perlindungan harta (*hifz al-māl*), salah satu tujuan utama syariat Islam (*maqāṣid al-syarī'ah*) (Eriyan dkk., 2026).

2.2.4 Faktor-faktor yang Mempengaruhi Penipuan Digital

Terjadinya penipuan digital dipengaruhi oleh berapa faktor, yaitu rendahnya literasi digital seringkali menjadi salah satu faktor utama yang menyebabkan seseorang lebih rentan terhadap kejahatan siber. Individu yang tidak memiliki pemahaman yang cukup mengenai keamanan digital cenderung mudah tertipu oleh berbagai modus penipuan seperti phishing, tautan palsu, maupun pesan yang mengatasnamakan lembaga resmi. Penelitian menunjukkan bahwa rendahnya literasi digital dapat meningkatkan risiko masyarakat menjadi korban penipuan digital karena kurangnya kemampuan dalam mengenali ancaman siber serta cara melindungi data pribadi di internet (Nisa dkk., 2025).

Literasi digital juga berperan dalam meningkatkan kemampuan individu dalam memverifikasi informasi yang beredar di internet. Individu dengan tingkat literasi digital yang baik cenderung lebih berhati-hati dalam memberikan informasi pribadi, tidak mudah percaya terhadap pesan yang mencurigakan, serta mampu mengidentifikasi indikasi penipuan digital (Harliani & Kurniawan, 2025).

Perkembangan teknologi informasi dan komunikasi telah menyebabkan semakin banyak data pribadi yang tersimpan dan diproses dalam sistem digital. Kondisi ini meningkatkan potensi terjadinya penyalahgunaan data apabila tidak diimbangi dengan sistem keamanan yang memadai. Penelitian menunjukkan bahwa kebocoran atau penyalahgunaan data pribadi dapat menjadi sarana bagi pelaku kejahatan untuk melakukan berbagai modus penipuan digital, seperti pencurian identitas, *phishing*, maupun pengambilalihan akun pengguna (Siahaan dkk., 2024).

Data pribadi nasabah perbankan sering menjadi target utama serangan siber karena informasi tersebut dapat digunakan untuk melakukan transaksi ilegal atau mengakses sistem keuangan secara tidak sah. Penelitian oleh Antoine dkk (2025) menunjukkan bahwa faktor manusia, serangan siber, serta lemahnya penerapan prosedur keamanan dapat menyebabkan kebocoran data pribadi yang pada akhirnya meningkatkan risiko penipuan digital pada nasabah perbankan.

2.2.5 Jenis-jenis Penipuan Digital

Penipuan digital memiliki berbagai bentuk, namun dalam konteks layanan perbankan digital, menurut penelitian Syafitri & Agustin (2023), *social engineering* merupakan salah satu bentuk serangan siber yang sering terjadi pada sektor perbankan. Nur (2025) menjelaskan bahwa penipuan digital dengan modus *social engineering* sering digunakan dalam kejahatan perbankan. Pelaku biasanya menyamar sebagai pihak bank dan melakukan manipulasi terhadap korban untuk memperoleh informasi rahasia, seperti kode OTP dan data pribadi lainnya. Temuan ini menunjukkan bahwa *social engineering* merupakan salah satu bentuk penipuan digital yang umum terjadi dan menjadi ancaman bagi nasabah perbankan. Oleh karena itu, penelitian ini memfokuskan jenis-jenis penipuan digital pada bentuk-bentuk *social engineering* yang umum menargetkan nasabah perbankan, yaitu *phishing*, *vishing*, *impersonation*, dan *baiting*.

Social engineering merupakan teknik manipulasi psikologis yang digunakan untuk mempengaruhi individu agar mengungkapkan informasi rahasia atau melakukan tindakan tertentu yang menguntungkan pelaku. Berbeda dengan serangan *cyber* konvensional yang memanfaatkan kelemahan teknis sistem keamanan, *social engineering* menargetkan faktor manusia sebagai titik lemah dalam sistem keamanan informasi. Melalui eksploitasi karakteristik dasar manusia seperti rasa percaya, keinginan untuk membantu, rasa takut, dan kecerobohan, pelaku kejahatan berhasil

memperoleh akses ke informasi pribadi, keuangan, atau sistem yang seharusnya terlindungi (Nur, 2025).

Menurut Fadillah dkk (2024), *phishing* merupakan bentuk penipuan yang bertujuan mencuri informasi pribadi pengguna melalui berbagai cara, seperti pembuatan situs web palsu, pengiriman email yang dimanipulasi, penggunaan tautan berbahaya, maupun penyebaran *malware*. Fadillah dkk (2024)) juga menjelaskan bahwa terjadinya serangan *phishing* dipengaruhi oleh beberapa faktor, antara lain rendahnya pengetahuan pengguna, kelemahan sistem keamanan, dan aspek psikologis yang dimanfaatkan oleh pelaku.

Vishing atau *voice phishing* adalah jenis serangan yang dilakukan melalui panggilan telepon dan sering dikenali sebagai fake call. Pelaku ingin mengeksploitasi emosi korban dengan melaporkan hal mendesak atau memberikan kabar baik, lalu saat korban sedang dalam pengaruh manipulasi pelaku akan meminta korban untuk memberikan data pribadinya (Anindya dkk., 2023).

Impersonation atau peniruan adalah teknik dasar yang digunakan pelaku *social engineering* agar tidak terlihat mencurigakan. Pelaku dapat menyamar sebagai pihak berwajib, petugas, hingga sebagai orang biasa yang perlu bantuan. *Impersonation* merupakan terapan dari prinsip dasar *social engineering*, yaitu untuk tampil sebagai non-hacker yang berhak atas informasi rahasia (Anindya dkk., 2023).

Anindya dkk (2023) menjelaskan bahwa *baiting* merupakan jenis serangan yang menggunakan umpan (bait) untuk menarik korban ke dalam jebakan yang dapat mencuri informasi rahasia hingga menginfeksi perangkat dengan malware. Umpan yang digunakan bisa berbentuk fisik, misalnya USB drive yang terkontaminasi malware diletakkan sembarangan menunggu untuk diakses oleh calon korban yang penasaran, dan umpan bentuk digital, misalnya saat korban ingin mengunduh suatu file dari internet, korban diminta untuk mengizinkan permintaan izin akses ke perangkat.

2.2.6 Indikator Penipuan Digital

Penipuan digital merupakan salah satu bentuk kejahatan siber yang paling sering terjadi dalam layanan perbankan digital, khususnya melalui metode *Social Engineering*. Dalam penelitian ini, variabel penipuan digital diukur melalui beberapa indikator yang diadaptasi dari konsep *Social Engineering* sebagaimana dijelaskan oleh Efendi dkk (2025). Penelitian tersebut mengacu pada teori *social engineering* yang dikemukakan oleh Mitnick dan Simon, serta disesuaikan dengan konteks perbankan digital. *Social engineering* merupakan metode manipulasi psikologis yang dilakukan untuk mengecoh pengguna agar memberikan informasi rahasia atau melakukan tindakan yang dapat merugikan dirinya sendiri. Oleh karena itu, indikator dalam penelitian ini difokuskan pada aspek kewaspadaan, kesadaran, dan pengetahuan pengguna

terhadap berbagai bentuk rekayasa sosial digital. Indikator penipuan digital pada penelitian ini meliputi:

1. Kewaspadaan terhadap berbagai bentuk rekayasa sosial digital.

Indikator ini menggambarkan kemampuan pengguna untuk mengenali berbagai upaya manipulasi yang dilakukan pelaku penipuan digital, seperti permintaan data pribadi, kode OTP, PIN, kata sandi, maupun tautan yang mencurigakan dan mengatasnamakan pihak tertentu.

2. Kesadaran terhadap berbagai bentuk rekayasa sosial digital.
Indikator ini menunjukkan tingkat kesadaran pengguna bahwa berbagai aktivitas digital, khususnya dalam layanan perbankan, memiliki potensi ancaman penipuan sehingga diperlukan sikap hati-hati dalam menerima informasi maupun melakukan transaksi.

3. Pengetahuan pengguna terhadap berbagai bentuk rekayasa sosial digital.

Indikator ini berkaitan dengan pemahaman pengguna mengenai berbagai modus penipuan digital yang berkembang, seperti *phishing*, *vishing*, *smishing*, penyalahgunaan identitas, dan berbagai bentuk rekayasa sosial lainnya yang bertujuan memperoleh informasi atau keuntungan secara ilegal.

2.3 Literasi Digital

2.3.1 Pengertian Literasi Digital

Literasi digital merupakan kemampuan dalam memahami, menggunakan, dan mengevaluasi informasi yang tersedia dalam bentuk digital dengan cara yang kritis dan etis. Literasi ini mencakup keterampilan teknis, pemahaman kritis terhadap konten, serta kemampuan berkomunikasi dan berkolaborasi menggunakan teknologi digital (Hobbs, 2017).

Dalam penelitian yang dilakukan oleh Kurnia dkk (2022) menyatakan literasi digital adalah pondasi membangun pola pikir dan kecakapan menghadapi tantangan era digital. Dalam konteks penipuan digital, edukasi literasi digital diperlukan untuk mengaktifkan kewaspadaan masyarakat melalui pemahaman menyeluruh dari hulu-hilir tentang penipuan digital.

2.3.2 Faktor-faktor yang Mempengaruhi Literasi Digital

Literasi digital tentunya dipengaruhi beberapa faktor diantaranya; penggunaan media online, nilai akademik, peran orangtua/keluarga, intensitas membaca. Intensitas media online berpengaruh positif terhadap kemampuan literasi digital, sehingga perlu diperhatikan fasilitas yang dikembangkan pemerintah dalam menunjang hal tersebut seperti memperhatikan aksesibilitas internet dan pelayanan akademik secara digital. Prestasi akademik berpengaruh secara signifikan terhadap kemampuan literasi digital, sehingga perlu pemahaman khusus bahwa dimensi akademik

ataupendidikan menjadi hal penting dalam memahami literasi digital. Intensitas membaca mempengaruhi kemampuan literasi digital secara signifikan. Hal ini menjadikan indikasi bahwa intensitas membaca merupakan pintu utama dalam mengelola kemampuan literasi apapun (Sitompul, 2024).

2.3.3 Aspek-aspek Literasi Digital

Aspek-aspek kompetensi literasi digital dalam buku *DigComp 3.0: European Digital Competence Framework* diterjemahkan menjadi 5 dimensi utama. Pertama, pencarian, evaluasi, dan pengelolaan informasi yang mencakup kemampuan menemukan, menilai, dan mengelola informasi digital secara kritis. Kedua, komunikasi dan kolaborasi yang berkaitan dengan interaksi, partisipasi, serta pengelolaan identitas digital dalam lingkungan daring. Ketiga, pembuatan konten digital yang meliputi kemampuan menciptakan dan mengembangkan konten secara kreatif dan bertanggung jawab dengan memperhatikan aspek hak cipta. Keempat, keamanan, kesejahteraan, dan penggunaan yang bertanggung jawab yang menekankan perlindungan data, keamanan perangkat, serta kesadaran terhadap dampak teknologi. Kelima, identifikasi dan pemecahan masalah yang berfokus pada kemampuan menyelesaikan masalah dan beradaptasi dengan perkembangan teknologi digital. Kelima dimensi ini membentuk kerangka komprehensif kompetensi literasi digital (Cosgrove & Cachia, 2025).

Penggunaan kerangka *DigComp* juga telah diterapkan dalam penelitian empiris di Indonesia untuk mengukur kompetensi literasi digital. Penelitian menunjukkan bahwa tingkat literasi digital dapat dianalisis melalui lima dimensi tersebut, yang mencakup kemampuan mengakses informasi, berkomunikasi secara digital, menciptakan konten, menjaga keamanan digital, serta menyelesaikan masalah berbasis teknologi (Wiguna dkk., 2023).

Dimensi *information* berkaitan dengan kemampuan individu dalam mencari, mengevaluasi, dan mengelola informasi digital secara kritis, yang menjadi dasar dalam pengambilan keputusan di era informasi (Jannah dkk., 2024). Dimensi *communication* menekankan pentingnya kemampuan berinteraksi dan berkolaborasi melalui media digital dengan memperhatikan etika komunikasi (Wiguna dkk., 2023).

Dimensi *content creation* mencerminkan kemampuan dalam menghasilkan dan memodifikasi konten digital secara kreatif, sedangkan dimensi *safety* berfokus pada perlindungan data pribadi, keamanan perangkat, serta kesadaran terhadap risiko digital (Ariani dkk., 2023). Adapun dimensi *problem solving* berkaitan dengan kemampuan individu dalam menyelesaikan masalah teknis serta beradaptasi dengan perkembangan teknologi digital yang dinamis (Wiguna dkk., 2023).

2.3.4 Tingkatan Literasi Digital

Terdapat tiga tingkatan pada literasi digital. Pertama, kompetensi digital yang meliputi keterampilan, konsep, pendekatan, dan perilaku. Kedua, penggunaan digital yang merujuk pada pengaplikasian kompetensi digital yang berhubungan dengan konteks tertentu. Ketiga, transformasi digital yang membutuhkan kreativitas dan inovasi pada dunia digital (Rizal dkk., 2022).

Kompetensi digital merupakan fondasi awal dalam literasi digital yang mencakup keterampilan teknis, pemahaman konsep, pendekatan penggunaan teknologi, serta perilaku dalam lingkungan digital. Pada tahap ini, individu dituntut untuk mampu mengoperasikan perangkat digital, memahami fungsi dasar teknologi informasi, serta memiliki sikap yang tepat dalam menggunakan media digital. Kompetensi digital tidak hanya bersifat mekanis, tetapi juga mencakup kemampuan memahami informasi secara dasar serta kesadaran terhadap etika penggunaan teknologi (Rizal dkk., 2022).

Penggunaan digital merujuk pada kemampuan individu dalam mengaplikasikan kompetensi digital yang dimiliki ke dalam berbagai konteks kehidupan, seperti pendidikan, pekerjaan, maupun interaksi sosial. Pada tahap ini, individu tidak lagi sekadar menggunakan teknologi, tetapi mampu memanfaatkannya secara efektif dan efisien sesuai dengan kebutuhan tertentu. Penggunaan digital juga melibatkan kemampuan memilih informasi yang

relevan, berkomunikasi secara digital, serta berkolaborasi melalui berbagai platform teknologi (Rizal dkk., 2022).

Transformasi digital merupakan tingkatan tertinggi dalam literasi digital yang menekankan pada kemampuan individu untuk menciptakan inovasi dan menghasilkan nilai tambah melalui teknologi digital. Pada tahap ini, individu dituntut untuk memiliki kreativitas, kemampuan berpikir kritis, serta keterampilan *problem solving* dalam memanfaatkan teknologi. Transformasi digital tidak hanya berfokus pada penggunaan teknologi, tetapi juga pada kemampuan untuk mengubah cara kerja, pola pikir, serta menghasilkan solusi baru yang berdampak luas dalam berbagai bidang kehidupan (Rizal dkk., 2022).

2.3.5 Indikator Literasi Digital

Literasi digital merupakan kemampuan individu dalam menggunakan teknologi digital untuk memperoleh, memahami, dan mengelola informasi secara efektif. Dalam penelitian yang dilakukan oleh Amri dkk (2024), indikator literasi digital diukur berdasarkan empat kompetensi utama yang mencerminkan kemampuan operasional dan kognitif dalam penggunaan media digital. Indikator literasi digital meliputi:

1. Pencarian di Internet (*Internet Searching*)

Indikator ini mengacu pada kemampuan individu dalam mencari informasi melalui mesin pencari dengan menggunakan kata kunci yang tepat. Kemampuan ini menunjukkan

keterampilan dasar dalam mengakses informasi digital secara efektif.

2. Navigasi Hypertext (*Hypertextual Navigation*)

Merupakan kemampuan individu dalam memahami dan menavigasi struktur informasi digital, seperti penggunaan hyperlink dan halaman website. Individu yang memiliki kemampuan ini dapat menjelajahi informasi digital dengan baik tanpa mengalami kebingungan.

3. Evaluasi Konten Informasi (*Content Evaluation*)

Indikator ini menunjukkan kemampuan individu dalam menilai kualitas dan kredibilitas informasi yang diperoleh dari internet. Individu mampu membandingkan berbagai sumber informasi untuk mendapatkan data yang lebih akurat dan terpercaya.

4. Penyusunan Pengetahuan (*Knowledge Assembly*)

Menggambarkan kemampuan individu dalam mengolah dan mengintegrasikan informasi dari berbagai sumber menjadi pengetahuan yang utuh. Individu tidak hanya mengumpulkan informasi, tetapi juga mampu menggunakannya untuk mendukung pembelajaran atau pengambilan keputusan.

Keempat indikator ini dinilai relevan karena mencerminkan kemampuan dasar hingga lanjutan dalam literasi digital, khususnya dalam menghadapi informasi di era digital.

2.4 Keamanan Data Pribadi

2.4.1 Pengertian Keamanan Data Pribadi

Keamanan data pribadi adalah upaya untuk melindungi informasi pribadi dari kerusakan, pencurian, atau akses yang tidak sah. Privasi digital adalah hak masing-masing orang untuk mengatur penggunaan data pribadinya di internet. Keduanya saling berhubungan dan menjadi dasar penting dalam mempertahankan keamanan di dunia digital. (Putra dkk., 2025).

Pengertian keamanan yaitu suatu proteksi atau perlindungan pada sumber-sumber fisik dan konseptual dari bahaya alam atau manusia. Keamanan terhadap sumber konseptual meliputi data dan informasi. Isu teratas dalam lingkungan e-commerce saat ini, yaitu privasi dan masalah keamanan pada data pribadi. Data pribadi seperti nama, alamat, nomor telepon, dan informasi keuangan bisa dengan mudah dicuri atau disalahgunakann oleh pihak yang tidak bertanggung jawab. Ancaman keamanan data pribadi pada pengguna *e-commerce* sangatlah beragam, termasuk serangan *malware*, *phishing*, *hacking*, dan pencurian identitas. Risiko yang ditimbulkan dari pelanggaran keamanan data pribadi tidak hanya dapat merugikan pengguna secara finansial, namun juga dapat merusak reputasi pengguna di masyarakat (Kehista dkk., 2023).

2.4.2 Jenis-jenis Data Pribadi

Data pribadi merupakan segala bentuk informasi yang dapat digunakan untuk mengidentifikasi seseorang baik secara langsung

maupun tidak langsung. Data pribadi tidak hanya terbatas pada identitas dasar, tetapi juga mencakup berbagai informasi yang berkaitan dengan aktivitas dan karakteristik individu (Suari & Sarjana, 2023).

Data pribadi dapat diklasifikasikan menjadi dua jenis utama, yaitu:

1. Data Pribadi Umum, yaitu data yang bersifat umum dan tidak sensitif, seperti: Nama lengkap, Jenis kelamin, Kewarganegaraan, Alamat tempat tinggal.
2. Data Pribadi Spesifik (Sensitif), yaitu data yang bersifat rahasia dan memerlukan perlindungan lebih tinggi, seperti: Data kesehatan, Data biometrik (sidik jari, wajah), Data keuangan, Riwayat transaksi, Data terkait keyakinan atau preferensi pribadi.

Klasifikasi ini penting karena tingkat perlindungan terhadap data pribadi berbeda tergantung pada tingkat sensitivitasnya. Data sensitif memiliki potensi risiko yang lebih tinggi apabila disalahgunakan, terutama dalam konteks kejahatan digital seperti penipuan berbasis data (Suvil dkk., 2024).

2.4.3 Prinsip Perlindungan Data Pribadi

Prinsip perlindungan data pribadi merupakan pedoman dasar dalam setiap proses pengelolaan data, mulai dari pengumpulan, pengolahan, hingga pemusnahan data. Prinsip ini berfungsi untuk menjamin perlindungan hak privasi individu sekaligus mencegah terjadinya penyalahgunaan data pribadi.

Dalam konteks hukum perlindungan data, setiap tahapan siklus data wajib memperhatikan prinsip-prinsip tersebut agar tercipta sistem perlindungan yang komprehensif dan berkelanjutan (Fikri & Rusdiana, 2023).

Prinsip perlindungan data pribadi mengacu pada standar internasional, terutama yang diatur dalam General Data Protection Regulation (GDPR). Prinsip-prinsip tersebut kemudian diadopsi ke dalam berbagai sistem hukum nasional, termasuk di Indonesia melalui Undang-Undang Pelindungan Data Pribadi. Hal ini menunjukkan bahwa perlindungan data pribadi telah berkembang menjadi standar global yang menjadi rujukan dalam pembentukan regulasi nasional (Pradana & Saragih, 2024).

Salah satu prinsip utama adalah legalitas, keadilan, dan transparansi (*lawfulness, fairness, and transparency*), yang menegaskan bahwa pemrosesan data harus dilakukan secara sah, adil, dan terbuka kepada subjek data. Dalam hal ini, pengolahan data harus didasarkan pada persetujuan yang jelas dari pemilik data, sehingga subjek data memiliki kontrol terhadap informasi pribadinya dan terhindar dari potensi penyalahgunaan (Pradana & Saragih, 2024).

Prinsip pembatasan tujuan (*purpose limitation*) mengharuskan bahwa data pribadi hanya diproses sesuai dengan tujuan awal pengumpulannya. Prinsip ini bertujuan untuk mencegah penggunaan data di luar kepentingan yang telah disepakati. Sejalan dengan itu, prinsip minimalisasi data (*data*

minimization) menegaskan bahwa data yang dikumpulkan harus relevan, memadai, dan terbatas pada kebutuhan tertentu, sehingga dapat meminimalkan risiko penyalahgunaan data (Fikri & Rusdiana, 2023).

Prinsip berikutnya adalah akurasi (*accuracy*), yang mengharuskan data pribadi selalu akurat dan diperbarui apabila diperlukan. Ketidakakuratan data dapat menimbulkan kerugian bagi subjek data, sehingga pembaruan data menjadi kewajiban bagi pengendali data. Selain itu, prinsip pembatasan penyimpanan (*storage limitation*) menyatakan bahwa data tidak boleh disimpan lebih lama dari yang diperlukan sesuai dengan tujuan pemrosesan (Fikri & Rusdiana, 2023).

Dalam aspek keamanan terdapat prinsip integritas dan kerahasiaan (*integrity and confidentiality*) yang mengharuskan adanya perlindungan terhadap data dari akses yang tidak sah, kehilangan, maupun kerusakan. Prinsip ini menuntut pengendali data untuk menerapkan sistem keamanan yang memadai. Dalam praktiknya, meningkatnya kasus kebocoran data menunjukkan bahwa perlindungan data tidak hanya bersifat normatif, tetapi juga memerlukan dukungan teknis berupa sistem keamanan informasi yang kuat (Rahman, 2021).

Terdapat prinsip akuntabilitas (*accountability*), yaitu kewajiban bagi pengendali data untuk bertanggung jawab atas seluruh proses pengolahan data serta mampu membuktikan kepatuhan terhadap prinsip-prinsip perlindungan data. Prinsip ini

merupakan inti dalam perlindungan data pribadi karena berfungsi sebagai mekanisme pengawasan terhadap penerapan seluruh prinsip lainnya (Pradana & Saragih, 2024).

Prinsip-prinsip perlindungan data pribadi tidak hanya berfungsi sebagai pedoman teknis, tetapi juga sebagai dasar normatif dan etis dalam sistem hukum. Prinsip-prinsip tersebut menjadi tolak ukur dalam menilai kepatuhan serta menjembatani kepentingan individu dan negara dalam pemanfaatan data pribadi. Negara memiliki peran penting dalam menjamin keseimbangan antara perlindungan privasi individu dan kebutuhan penggunaan data untuk pelayanan publik (Rahman, 2021).

2.4.4 Risiko Kebocoran Data Pribadi

Kebocoran data pribadi merupakan salah satu ancaman utama dalam era digital yang ditandai dengan meningkatnya penggunaan teknologi informasi dalam berbagai aspek kehidupan. Peristiwa ini terjadi ketika informasi individu diakses, digunakan, atau disebarluaskan tanpa persetujuan pemiliknya, baik akibat kelemahan sistem maupun tindakan pihak yang tidak berwenang. Kondisi tersebut berpotensi menimbulkan kerugian serta mengancam hak privasi yang seharusnya dilindungi (Azzahra & Nurkhaerani, 2024).

Perkembangan teknologi seperti *big data*, *cloud computing*, dan *Internet of Things* (IoT) turut meningkatkan kompleksitas ancaman terhadap keamanan informasi. Sistem yang saling

terintegrasi serta pengolahan data dalam jumlah besar membuka peluang munculnya celah keamanan yang dapat dimanfaatkan oleh pihak tertentu. Selain itu, lemahnya pengamanan sistem dan kurangnya pengawasan menjadi faktor utama meningkatnya insiden pelanggaran data di Indonesia (Mulyadi dkk., 2026).

Aspek manusia (*human error*) dan rendahnya literasi digital masyarakat juga berkontribusi terhadap tingginya potensi kebocoran. Kurangnya pemahaman mengenai pentingnya menjaga informasi pribadi menyebabkan individu sering kali secara tidak sadar membagikan data sensitif di ruang digital. Hal ini meningkatkan peluang penyalahgunaan oleh pihak yang tidak bertanggung jawab (Prasetya dkk., 2025).

Dampak dari kebocoran informasi tidak hanya dirasakan oleh individu, tetapi juga meluas ke aspek sosial dan ekonomi. Salah satu konsekuensi yang umum terjadi adalah pencurian identitas (*identity theft*), yaitu penggunaan informasi pribadi tanpa izin untuk kepentingan tertentu, seperti penipuan atau akses ilegal terhadap layanan digital. Selain itu, insiden semacam ini juga dapat memicu berbagai bentuk kejahatan siber lainnya (Azzahra & Nurkhaerani, 2024).

Organisasi yang mengalami insiden serupa berisiko kehilangan kepercayaan publik, menghadapi kerugian finansial, serta menerima konsekuensi hukum akibat kelalaian dalam melindungi data. Hal ini menunjukkan bahwa tanggung jawab

perlindungan tidak hanya berada pada individu, tetapi juga pada institusi sebagai pengelola informasi (Bua & Idris, 2025).

Penyalahgunaan data dapat terjadi untuk kepentingan komersial maupun politik, seperti *profiling*, *targeted advertising*, hingga manipulasi opini publik. Praktik tersebut berpotensi menciptakan ketimpangan informasi serta mengancam kebebasan individu dalam ruang digital, sehingga memperluas dampak kebocoran ke ranah sosial yang lebih kompleks (Bua & Idris, 2025).

Risiko kebocoran data pribadi merupakan tantangan serius yang memerlukan penanganan secara menyeluruh. Upaya mitigasi dapat dilakukan melalui penguatan sistem keamanan, peningkatan literasi digital masyarakat, serta penegakan regulasi yang tegas. Pendekatan yang terintegrasi antara aspek hukum, teknis, dan sosial menjadi kunci dalam meminimalkan ancaman di era digital (Mulyadi dkk., 2026).

2.4.5 Indikator Keamanan Data Pribadi

Indikator keamanan data pribadi mengacu pada konsep CIA Triad (*Confidentiality, Integrity, Availability*) yang merupakan model terkenal untuk pengembangan kebijakan keamanan, digunakan untuk mengidentifikasi masalah dan solusi yang diperlukan untuk keamanan dan sistem informasi. Model ini banyak digunakan sebagai standar dalam menilai keamanan sistem

informasi karena mampu mencakup aspek perlindungan data secara menyeluruh (Harahap dkk., 2023).

Indikator keamanan data pribadi dalam penelitian ini dirumuskan sebagai berikut:

1. Kerahasiaan (*Confidentiality*)

Kerahasiaan merupakan upaya untuk memastikan bahwa data pribadi hanya dapat diakses oleh pihak yang berwenang dan tidak diungkapkan kepada pihak lain tanpa izin.

2. Integritas (*Integrity*)

Integritas adalah kemampuan untuk menjaga keakuratan, konsistensi, dan keutuhan data sehingga tidak dapat diubah, dimodifikasi, atau dihapus tanpa otorisasi.

3. Ketersediaan (*Availability*)

Ketersediaan merupakan jaminan bahwa data pribadi dapat diakses oleh pihak yang berhak kapan saja saat dibutuhkan tanpa hambatan.

2.5 Penelitian Terdahulu

Harliani & Kurniawan^N (2025) melakukan penelitian berjudul “Pengaruh Kemampuan Literasi Digital Terhadap Pencegahan Penipuan Online Pada Remaja Desa Saentis”. Metode penelitian yang digunakan adalah pendekatan kuantitatif dengan jenis penelitian *ex post facto*, pengumpulan data melalui angket kepada 38 responden remaja berusia 13–19 tahun yang dipilih secara *purposive sampling*, dan analisis data menggunakan

deskriptif serta regresi linear sederhana. Hasil penelitian menunjukkan bahwa sebanyak 76,3% remaja memiliki kemampuan literasi digital dalam kategori sangat baik, sedangkan tingkat penipuan online remaja berada pada kategori sangat tinggi (68,5%). Berdasarkan uji regresi linear sederhana, diperoleh nilai signifikansi 0,000 dan nilai R Square sebesar 0,632, yang artinya kemampuan literasi digital memberikan pengaruh sebesar 63,2% terhadap variasi pencegahan penipuan online remaja.

Nupus (2025) melakukan penelitian berjudul "Pengaruh *Cyber Crime* dan Persepsi Keamanan terhadap Tingkat Kepercayaan Pengguna Produk E-banking (Survei pada Pengguna E-banking Bank Syariah di Indonesia)". Penelitian ini bertujuan untuk menganalisis seberapa besar pengaruh *cyber crime* dan persepsi keamanan terhadap tingkat kepercayaan pengguna produk e-banking pada bank syariah di Indonesia. Metode yang digunakan adalah pendekatan kuantitatif dengan survei kuesioner dan analisis regresi linear berganda. Hasil penelitian menunjukkan bahwa *cyber crime* dan persepsi keamanan berpengaruh signifikan terhadap tingkat kepercayaan pengguna produk e-banking bank syariah.

Efendi dkk (2025) melakukan penelitian berjudul "Pengaruh *Social Engineering* dan *Cyber Crime* terhadap Persepsi Keamanan pada Aplikasi BSI Mobile". Penelitian ini bertujuan untuk mengetahui pengaruh *social engineering* dan *cyber crime* terhadap persepsi keamanan pengguna aplikasi BSI Mobile di tengah meningkatnya kasus kejahatan siber yang menasar layanan

perbankan digital. Metode penelitian yang digunakan adalah pendekatan kuantitatif dengan metode survei terhadap 100 responden pengguna aktif aplikasi BSI Mobile menggunakan analisis regresi linear berganda. Hasil penelitian menunjukkan bahwa baik *social engineering* maupun *cyber crime* masing-masing berpengaruh signifikan secara parsial maupun simultan terhadap persepsi keamanan pengguna.

Yoviani dkk (2025) melakukan penelitian berjudul “Pengaruh Kemudahan, Keamanan dan Literasi Digital terhadap Minat Nasabah Menggunakan Aplikasi Muamalat DIN”. Penelitian ini bertujuan untuk mengetahui pengaruh kemudahan, keamanan, dan literasi digital terhadap minat nasabah Bank Muamalat dalam menggunakan aplikasi Muamalat DIN (*Digital Islamic Network*) sebagai layanan mobile banking syariah. Metode penelitian yang digunakan adalah pendekatan kuantitatif dengan survei kuesioner, teknik *purposive sampling* terhadap 100 responden nasabah Bank Muamalat di wilayah Sukabumi, dan analisis data menggunakan regresi linear berganda. Hasil penelitian menunjukkan bahwa kemudahan, keamanan, dan literasi digital masing-masing berpengaruh positif dan signifikan secara parsial maupun simultan terhadap minat nasabah dalam menggunakan aplikasi Muamalat DIN.

Sembiring dkk (2024) melakukan penelitian berjudul "Pengaruh Ancaman Siber *Ransomware* dan Gangguan Sistem Layanan Mobile Banking terhadap Kepercayaan Nasabah pada

Bank BSI KCP Kisaran". Penelitian ini bertujuan untuk menguji pengaruh ancaman *cyber ransomware* dan gangguan sistem layanan mobile banking terhadap kepercayaan nasabah. Metode penelitian yang digunakan adalah pendekatan kuantitatif dengan distribusi kuesioner dan analisis regresi linear berganda. Hasil penelitian menunjukkan bahwa ancaman *cyber ransomware* dan gangguan yang sering terjadi pada sistem layanan mobile banking berpengaruh negatif signifikan sehingga menurunkan kepercayaan nasabah BSI KCP Kisaran.

Hutagaol dkk (2024) melakukan penelitian berjudul "Identifikasi Tingkat Kesadaran Pengguna Mobile Banking terhadap Ancaman *Cyber crime*". Penelitian ini bertujuan untuk mengidentifikasi tingkat kesadaran pengguna mobile banking terhadap berbagai ancaman *cyber crime* berdasarkan tingkat pengetahuan keamanan siber dan perilaku pengguna. Metode penelitian yang digunakan adalah pendekatan kuantitatif deskriptif dengan survei kuesioner terstruktur serta analisis regresi linier berganda. Hasil penelitian menunjukkan bahwa tingkat pengetahuan keamanan siber dan perilaku praktik keamanan pengguna berpengaruh positif dan signifikan terhadap persepsi risiko ancaman *cyber crime*.

Amzah dkk (2024) melakukan penelitian berjudul "Analisis Pengaruh Kualitas Layanan dan Persepsi *Cyber crime* terhadap Loyalitas Nasabah Pengguna E-Banking pada Bank Syariah Indonesia Kota Jambi". Penelitian ini bertujuan untuk menganalisis

pengaruh kualitas layanan dan persepsi *cyber crime* terhadap loyalitas nasabah pengguna e-banking BSI. Metode penelitian yang digunakan adalah pendekatan kuantitatif dengan survei kuesioner, teknik *purposive sampling*, dan analisis regresi linear berganda. Hasil penelitian menunjukkan bahwa persepsi *cyber crime* berpengaruh negatif signifikan terhadap loyalitas nasabah pengguna e-banking BSI; semakin tinggi persepsi ancaman *cyber crime* maka semakin rendah loyalitas nasabah.

Permana dkk (2024) melakukan penelitian berjudul "Pengaruh Keamanan Data Pribadi terhadap Kepercayaan Pengguna di Era Transformasi Digital: Studi Kasus pada Aplikasi Mobile Banking". Penelitian ini bertujuan untuk menguji bagaimana kepercayaan pengguna terhadap aplikasi mobile banking dipengaruhi oleh persepsi keamanan data pribadi. Metode penelitian yang digunakan adalah pendekatan kuantitatif dengan survei kuesioner skala likert kepada 30 responden yang dipilih secara acak serta dianalisis menggunakan regresi linear sederhana. Hasil penelitian menunjukkan korelasi positif yang kuat antara kepercayaan pengguna dan persepsi keamanan data pribadi, di mana sistem verifikasi berbasis teknologi seperti OTP dan biometrik memiliki dampak terbesar terhadap persepsi keamanan.

Erfiana & Anwar (2023) melakukan penelitian berjudul "Pengaruh *Cyber Crime* dan E-Banking terhadap Kepuasan Nasabah Bank Syariah Indonesia (Studi Kasus Mahasiswa Solo Raya)". Penelitian ini bertujuan untuk menganalisis pengaruh cyber

crime dan penggunaan e-banking terhadap kepuasan nasabah Bank Syariah Indonesia. Metode penelitian yang digunakan adalah pendekatan kuantitatif dengan survei kuesioner, teknik *purposive sampling*, dan analisis regresi linear berganda. Hasil penelitian menunjukkan bahwa *cyber crime* berpengaruh negatif signifikan terhadap kepuasan nasabah BSI, sementara penggunaan e-banking berpengaruh positif terhadap kepuasan nasabah.

Tiffani (2023) melakukan penelitian berjudul "Pengaruh Literasi Keuangan dan Literasi Digital terhadap Preferensi Bank Digital". Penelitian ini bertujuan untuk mengetahui dan memastikan hubungan antara literasi keuangan dan literasi digital dengan preferensi konsumen terhadap bank digital. Metode penelitian yang digunakan adalah deskriptif dengan pendekatan kuantitatif menggunakan data primer melalui kuesioner dan *convenience sampling* serta analisis regresi linear berganda. Hasil penelitian menunjukkan bahwa literasi keuangan dan literasi digital berpengaruh positif dan signifikan terhadap preferensi konsumen dalam menggunakan bank digital.

Tabel 2. 1 Penelitian Terdahulu

NO	Identitas Penelitian	Hasil Penelitian
1	Harliani & Kurniawan (2025) “Pengaruh Kemampuan Literasi Digital Terhadap Pencegahan Penipuan Online Pada Remaja Desa Saentis”	Hasil penelitian menunjukkan bahwa sebanyak 76,3% remaja memiliki kemampuan literasi digital dalam kategori sangat baik, sedangkan tingkat penipuan online remaja berada pada kategori sangat tinggi (68,5%). Berdasarkan uji regresi linear sederhana, diperoleh nilai signifikansi 0,000 dan nilai R Square sebesar 0,632, yang artinya

NO	Identitas Penelitian	Hasil Penelitian
		kemampuan literasi digital memberikan pengaruh sebesar 63,2% terhadap variasi pencegahan penipuan online remaja.
2	Nupus dkk (2025) “Pengaruh <i>Cyber Crime</i> dan Persepsi Keamanan terhadap Tingkat Kepercayaan Pengguna Produk E-banking (Survei pada Pengguna E-banking Bank Syariah di Indonesia)”	Hasil penelitian menunjukkan bahwa <i>cyber crime</i> dan persepsi keamanan berpengaruh signifikan terhadap tingkat kepercayaan pengguna produk e-banking bank syariah.
3	Efendi dkk (2025) “Pengaruh Social Engineering dan <i>Cyber Crime</i> terhadap Persepsi Keamanan pada Aplikasi BSI Mobile”	Hasil penelitian menunjukkan bahwa baik social engineering maupun <i>cyber crime</i> masing-masing berpengaruh signifikan secara parsial maupun simultan terhadap persepsi keamanan pengguna.
4	Yoviani dkk (2025) “Pengaruh Kemudahan, Keamanan dan Literasi Digital terhadap Minat Nasabah Menggunakan Aplikasi Muamalat DIN”	Hasil penelitian menunjukkan bahwa kemudahan, keamanan, dan literasi digital masing-masing berpengaruh positif dan signifikan secara parsial maupun simultan terhadap minat nasabah dalam menggunakan aplikasi Muamalat DIN.
5	Sembiring dkk (2024) “Pengaruh Ancaman Siber <i>Ransomware</i> dan Gangguan Sistem Layanan Mobile Banking terhadap Kepercayaan Nasabah pada Bank BSI KCP Kisaran”	Hasil penelitian menunjukkan bahwa ancaman <i>cyber ransomware</i> dan gangguan yang sering terjadi pada sistem layanan mobile banking berpengaruh negatif signifikan sehingga menurunkan kepercayaan nasabah BSI KCP Kisaran.
6	Hutagaol dkk (2024) “Identifikasi Tingkat Kesadaran Pengguna Mobile Banking terhadap Ancaman <i>Cyber Crime</i> ”	Hasil penelitian menunjukkan bahwa tingkat pengetahuan keamanan siber dan perilaku praktik keamanan pengguna berpengaruh positif dan signifikan terhadap persepsi risiko ancaman <i>cyber crime</i> .
7	Amzah (2024) “Analisis Pengaruh Kualitas Layanan dan Persepsi <i>Cyber Crime</i> terhadap Loyalitas Nasabah Pengguna E-Banking pada Bank Syariah Indonesia Kota Jambi”	Hasil penelitian menunjukkan bahwa persepsi <i>cyber crime</i> berpengaruh negatif signifikan terhadap loyalitas nasabah pengguna e-banking BSI; semakin tinggi persepsi ancaman <i>cyber crime</i> maka semakin rendah loyalitas nasabah.

NO	Identitas Penelitian	Hasil Penelitian
8	Permana dkk (2024) “Pengaruh Keamanan Data Pribadi terhadap Kepercayaan Pengguna di Era Transformasi Digital: Studi Kasus pada Aplikasi Mobile Banking”	Hasil penelitian menunjukkan korelasi positif yang kuat antara kepercayaan pengguna dan persepsi keamanan data pribadi, di mana sistem verifikasi berbasis teknologi seperti OTP dan biometrik memiliki dampak terbesar terhadap persepsi keamanan.
9	Erfiana (2023) “Pengaruh <i>Cyber Crime</i> dan E-Banking terhadap Kepuasan Nasabah Bank Syariah Indonesia (Studi Kasus Mahasiswa Solo Raya)”	Hasil penelitian menunjukkan bahwa <i>cyber crime</i> berpengaruh negatif signifikan terhadap kepuasan nasabah BSI, sementara penggunaan e-banking berpengaruh positif terhadap kepuasan nasabah.
10	Tiffani (2023) “Pengaruh Literasi Keuangan dan Literasi Digital terhadap Preferensi Bank Digital”	Hasil penelitian menunjukkan bahwa literasi keuangan dan literasi digital berpengaruh positif dan signifikan terhadap preferensi konsumen dalam menggunakan bank digital.

Penelitian Harliani & Kurniawan (2025) memiliki persamaan dengan penelitian ini karena sama-sama mengkaji literasi digital menggunakan pendekatan kuantitatif. Perbedaannya, penelitian tersebut berfokus pada pengaruh literasi digital terhadap pencegahan penipuan online pada remaja di Desa Saentis, sedangkan penelitian ini mengkaji pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

Penelitian Nupus dkk (2025) memiliki persamaan dengan penelitian ini karena sama-sama membahas keamanan dan layanan perbankan syariah menggunakan pendekatan kuantitatif. Perbedaannya, penelitian tersebut mengkaji pengaruh kejahatan

digital dan keamanan terhadap kepercayaan nasabah e-banking syariah, sedangkan penelitian ini berfokus pada pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital.

Penelitian Efendi dkk (2025) memiliki persamaan dengan penelitian ini karena sama-sama membahas ancaman kejahatan siber pada layanan perbankan syariah menggunakan metode kuantitatif. Perbedaannya, penelitian tersebut menguji pengaruh *social engineering* dan *cyber crime* terhadap persepsi keamanan pengguna BSI Mobile, sedangkan penelitian ini menguji pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah.

Penelitian Yoviani dkk (2025) memiliki persamaan dengan penelitian ini karena sama-sama mengkaji literasi digital dan keamanan menggunakan pendekatan kuantitatif. Perbedaannya, penelitian tersebut berfokus pada minat penggunaan aplikasi Muamalat DIN dengan menambahkan variabel kemudahan, sedangkan penelitian ini berfokus pada penipuan digital dengan variabel literasi digital dan keamanan data pribadi.

Penelitian Sembiring dkk (2024) memiliki persamaan dengan penelitian ini karena sama-sama membahas keamanan digital pada sektor perbankan syariah menggunakan pendekatan kuantitatif. Perbedaannya, penelitian tersebut berfokus pada pengaruh ancaman *ransomware* terhadap kepercayaan nasabah Bank Syariah Indonesia, sedangkan penelitian ini mengkaji

pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital.

Penelitian Hutagaol dkk (2024) memiliki persamaan dengan penelitian ini karena sama-sama membahas keamanan siber pada pengguna mobile banking menggunakan pendekatan kuantitatif. Perbedaannya, penelitian tersebut berfokus pada tingkat kesadaran (*cyber security awareness*) pengguna mobile banking terhadap ancaman kejahatan siber, sedangkan penelitian ini mengkaji pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

Penelitian Amzah dkk (2024) memiliki persamaan dengan penelitian ini karena sama-sama membahas keamanan layanan perbankan syariah dengan pendekatan kuantitatif. Perbedaannya, penelitian tersebut mengkaji pengaruh kualitas pelayanan, mobile banking, dan *cyber crime* terhadap loyalitas nasabah Bank Syariah Indonesia, sedangkan penelitian ini mengkaji pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital.

Penelitian Permana dkk (2024) memiliki persamaan dengan penelitian ini karena sama-sama mengkaji keamanan data pribadi pada layanan perbankan digital menggunakan pendekatan kuantitatif. Perbedaannya, penelitian tersebut berfokus pada kepercayaan pengguna mobile banking, sedangkan penelitian ini berfokus pada penipuan digital pada nasabah Bank Aceh Syariah.

Penelitian Erfiana (2023) memiliki persamaan dengan penelitian ini karena sama-sama membahas keamanan layanan perbankan syariah menggunakan metode kuantitatif. Perbedaannya, penelitian tersebut mengkaji pengaruh *cyber crime* terhadap kepuasan nasabah Bank Syariah Indonesia, sedangkan penelitian ini mengkaji pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah.

Penelitian Tiffani (2023) memiliki persamaan dengan penelitian ini karena sama-sama mengkaji literasi digital menggunakan pendekatan kuantitatif. Perbedaannya, penelitian tersebut berfokus pada pengaruh literasi digital terhadap preferensi penggunaan bank digital, sedangkan penelitian ini mengkaji pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

Tabel 2. 2 Persaman dan Perbedaan Penelitian Terdahulu

No	Nama Peneliti	Persamaan	Perbedaan
1	Harliani & Kurniawan (2025)	Sama-sama mengkaji pengaruh literasi digital terhadap pencegahan penipuan digital pada remaja dengan metode kuantitatif, pendekatan survei angket, <i>purposive sampling</i> .	Penelitian ini berfokus pada pencegahan penipuan online pada remaja di Desa Saentis, Deli Serdang, Sumatera Utara dengan satu variabel bebas (literasi digital), sedangkan penelitian penulis mengkaji pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital

No	Nama Peneliti	Persamaan	Perbedaan
			khusus pada nasabah Bank Aceh Syariah di Kota Banda Aceh
2	Nupus dkk (2025)	Sama-sama membahas pengaruh kejahatan digital dan keamanan terhadap nasabah perbankan syariah dengan pendekatan kuantitatif	Penelitian ini berfokus pada kepercayaan nasabah e-banking syariah secara umum, sedangkan penelitian penulis berfokus pada penipuan digital nasabah Bank Aceh Syariah di Kota Banda Aceh
3	Efendi dkk (2025)	Sama-sama membahas ancaman penipuan digital dan keamanan pada layanan perbankan syariah dengan metode kuantitatif	Penelitian ini berfokus pada pengaruh social engineering dan <i>cyber crime</i> terhadap persepsi keamanan, sedangkan penelitian penulis mengkaji literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital
4	Yoviani dkk (2025)	Sama-sama mengkaji pengaruh keamanan dan literasi digital terhadap perilaku nasabah perbankan syariah dengan metode kuantitatif dan analisis regresi linear berganda	Penelitian ini berfokus pada minat penggunaan aplikasi mobile banking syariah (Muamalat DIN) dengan tiga variabel bebas (kemudahan, keamanan, literasi digital) pada nasabah di Sukabumi, sedangkan penelitian penulis mengkaji pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Banda Aceh
5	Sembiring dkk (2024)	Sama-sama membahas dampak ancaman keamanan digital terhadap nasabah perbankan syariah dengan	Penelitian ini berfokus pada ancaman <i>ransomware</i> dan gangguan sistem terhadap kepercayaan nasabah BSI, sedangkan penelitian

No	Nama Peneliti	Persamaan	Perbedaan
		metode kuantitatif	penulis lebih fokus pada literasi digital dan keamanan data pribadi dalam mencegah penipuan digital
6	Hutagaol dkk (2024)	Sama-sama mengkaji hubungan antara literasi/pengetahuan digital dan keamanan dengan ancaman kejahatan siber pada pengguna perbankan digital	Penelitian ini berfokus pada identifikasi kesadaran pengguna mobile banking secara umum, sedangkan penelitian penulis menguji pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah
7	Amzah (2024)	Sama-sama membahas dampak kejahatan/ancaman digital terhadap nasabah perbankan syariah dengan pendekatan kuantitatif	Penelitian ini berfokus pada loyalitas nasabah BSI Kota Jambi, sedangkan penelitian penulis berfokus pada penipuan digital nasabah Bank Aceh Syariah di Banda Aceh
8	Permana dkk (2024)	Sama-sama mengkaji pengaruh keamanan data pribadi pada layanan perbankan digital dengan metode kuantitatif	Penelitian ini berfokus pada kepercayaan pengguna mobile banking, sedangkan penelitian penulis mengkaji penipuan digital pada nasabah Bank Aceh Syariah
9	Erfiana (2023)	Sama-sama membahas dampak kejahatan siber terhadap nasabah perbankan syariah dengan menggunakan metode kuantitatif	Penelitian ini berfokus pada kepuasan nasabah BSI mahasiswa Solo Raya, sedangkan penelitian penulis meneliti penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh
10	Tiffani (2023)	Sama-sama mengkaji pengaruh literasi	Penelitian ini berfokus pada preferensi

No	Nama Peneliti	Persamaan	Perbedaan
		digital terhadap perilaku dan keputusan pengguna layanan perbankan digital dengan metode kuantitatif	penggunaan bank digital, sedangkan penelitian penulis mengkaji pengaruh literasi digital terhadap kewaspadaan terhadap penipuan digital pada nasabah bank syariah

2.6 Hubungan Antar Variabel

Hubungan antar variabel dalam penelitian ini menjelaskan keterkaitan antara variabel independen, yaitu literasi digital (X1) dan keamanan data pribadi (X2), terhadap variabel dependen yaitu penipuan digital (Y). Hubungan ini dibangun berdasarkan landasan teori dan hasil penelitian terdahulu yang relevan.

2.6.1 Hubungan Literasi Digital terhadap Kewaspadaan terhadap Penipuan Digital

Literasi digital merupakan kemampuan individu dalam memahami, mengevaluasi, dan menggunakan teknologi digital secara bijak dan bertanggung jawab. Harliani & Kurniawan (2025) membuktikan bahwa kemampuan literasi digital berpengaruh signifikan terhadap pencegahan penipuan online, dengan nilai R Square sebesar 0,632 pada remaja yang diteliti. Selaras dengan itu, Tiffani (2023) menemukan bahwa literasi digital berpengaruh positif dan signifikan terhadap perilaku pengguna dalam memilih layanan digital, sedangkan Yoviani dkk (2025) menunjukkan bahwa literasi digital turut berpengaruh signifikan terhadap minat nasabah dalam menggunakan aplikasi perbankan syariah. Temuan-

temuan tersebut memperkuat dugaan bahwa literasi digital berpengaruh terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

2.6.2 Hubungan Keamanan Data Pribadi terhadap Kewaspadaan terhadap Penipuan Digital

Keamanan data pribadi merupakan upaya perlindungan terhadap informasi individu agar tidak disalahgunakan oleh pihak yang tidak bertanggung jawab. Nupus dkk (2025) membuktikan bahwa cyber crime dan persepsi keamanan berpengaruh signifikan terhadap tingkat kepercayaan pengguna e-banking bank syariah, sementara Permana dkk (2024) menemukan korelasi positif yang kuat antara kepercayaan pengguna dan persepsi keamanan data pribadi, di mana sistem verifikasi seperti OTP dan biometrik berperan besar dalam menekan risiko penipuan. Hutagaol dkk (2024) juga melaporkan bahwa tingkat pengetahuan keamanan siber dan perilaku praktik keamanan pengguna berpengaruh positif dan signifikan terhadap persepsi risiko cyber crime, sedangkan Sembiring dkk (2024) menunjukkan bahwa ancaman cyber ransomware dan gangguan sistem layanan berpengaruh negatif signifikan terhadap kepercayaan nasabah. Erfiana & Anwar (2023) turut menemukan bahwa cyber crime berpengaruh negatif signifikan terhadap kepuasan nasabah bank syariah. Hasil-hasil tersebut memperkuat dugaan bahwa keamanan data pribadi

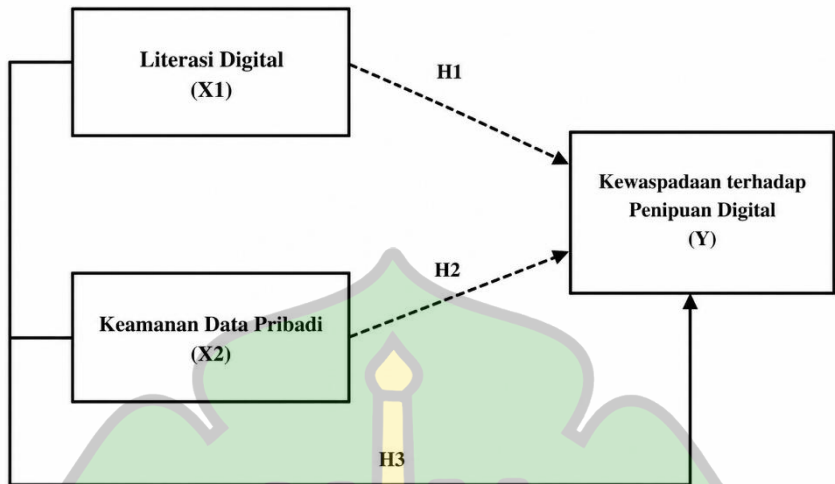
berpengaruh terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

2.6.3 Hubungan Literasi Digital dan Keamanan Data Pribadi terhadap Kewaspadaan terhadap Penipuan Digital

Literasi digital dan keamanan data pribadi memberikan pengaruh yang lebih kuat dalam menekan risiko penipuan digital dibandingkan jika hanya salah satu faktor saja. Kajian empiris terdahulu turut mendukung dugaan pengaruh simultan tersebut. Yoviani dkk (2025) membuktikan bahwa kemudahan, keamanan, dan literasi digital secara simultan berpengaruh positif dan signifikan terhadap minat nasabah dalam menggunakan aplikasi perbankan syariah, sedangkan Efendi dkk (2025) menemukan bahwa social engineering dan cyber crime secara simultan berpengaruh signifikan terhadap persepsi keamanan pengguna aplikasi mobile banking. Amzah dkk (2024) juga menunjukkan bahwa persepsi cyber crime, bersama faktor kualitas layanan, berpengaruh signifikan terhadap loyalitas nasabah pengguna e-banking. Temuan-temuan tersebut memperkuat dugaan bahwa literasi digital dan keamanan data pribadi secara simultan berpengaruh terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

2.7 Kerangka Berpikir

Diagram hubungan variabel penelitian:



Berdasarkan kerangka berpikir penelitian, Literasi Digital (X1) dan Keamanan Data Pribadi (X2) merupakan variabel independen yang memengaruhi kewaspadaan terhadap Penipuan Digital pada Nasabah Bank Aceh Syariah di Kota Banda Aceh (Y). H1 menunjukkan bahwa literasi digital diduga berpengaruh terhadap kewaspadaan terhadap penipuan digital, sedangkan H2 menunjukkan bahwa keamanan data pribadi diduga berpengaruh terhadap kewaspadaan terhadap penipuan digital. H3 menunjukkan bahwa literasi digital dan keamanan data pribadi secara simultan diduga berpengaruh terhadap kewaspadaan terhadap penipuan digital.

2.8 Hipotesis Penelitian

Hipotesis merupakan jawaban sementara untuk masalah penelitian yang diajukan sehingga dapat diuji (Ibrahim, 2023). Berikut merupakan hipotesis yang digunakan pada penelitian ini:

H1 : Literasi digital berpengaruh terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

H2 : Keamanan data pribadi berpengaruh terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

H3 : Literasi digital dan keamanan data pribadi secara simultan berpengaruh terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

BAB III

METODE PENELITIAN

3.1 Jenis Penelitian

Penelitian ini menggunakan pendekatan kuantitatif. Penelitian kuantitatif merupakan jenis penelitian yang menggunakan data berbentuk angka atau data yang dapat dikonversi ke dalam bentuk numerik melalui proses pengukuran tertentu. Data kuantitatif dapat berupa data diskrit (nominal) maupun data kontinum yang digunakan untuk menganalisis hubungan atau pengaruh antarvariabel dalam suatu penelitian. Dengan menggunakan pendekatan ini, peneliti dapat menguji hipotesis serta mengetahui hubungan maupun pengaruh variabel yang diteliti secara terukur dan sistematis (Ibrahim, 2023).

Penelitian ini bertujuan untuk mengetahui bagaimana pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh. Pengumpulan data dilakukan dengan menyebarkan kuesioner dan pengukuran dengan skala likert. Kuesioner terdiri dari pertanyaan yang sesuai dengan indikator yang telah ditetapkan.

3.2 Lokasi Dan Waktu Penelitian

Lokasi penelitian yang dipilih adalah Kota Banda Aceh. Objek penelitian difokuskan pada nasabah Bank Aceh Syariah di Kota Banda Aceh. Alasan pemilihan lokasi ini adalah karena Banda

Aceh merupakan ibu kota provinsi yang menjadi pusat aktivitas ekonomi dan keuangan di wilayah Aceh, sehingga mencerminkan perilaku masyarakat yang cukup representatif dalam hal penggunaan layanan perbankan syariah dan transaksi digital. Selain itu, meningkatnya kasus penipuan digital di lingkungan perbankan menjadikan Banda Aceh relevan sebagai lokasi penelitian, khususnya dalam mengkaji peran literasi digital dan keamanan data pribadi nasabah.

3.3 Populasi dan Sampel

3.3.1 Populasi

Menurut Sugiyono (2023) populasi merupakan wilayah generalisasi yang mencakup objek atau subjek dengan karakteristik tertentu yang telah ditetapkan oleh peneliti untuk dipelajari, sehingga dapat ditarik suatu kesimpulan. Dengan demikian, populasi dalam penelitian ini adalah seluruh nasabah Bank Aceh Syariah yang berdomisili di Kota Banda Aceh.

3.3.2 Sampel

Sampel adalah bagian dari populasi yang memiliki karakteristik tertentu dan digunakan untuk mewakili populasi dalam penelitian. Penelitian ini menggunakan teknik *nonprobability sampling* dengan metode *purposive sampling*, artinya setiap anggota populasi tidak memiliki kesempatan atau peluang yang sama sebagai sampel (Ibrahim, 2023).

Karakteristik responden ditetapkan untuk memastikan sampel sesuai dengan tujuan penelitian dan relevan dengan variabel yang diteliti. Karakteristik responden dalam penelitian ini meliputi:

1. Nasabah Bank Aceh Syariah
2. Memiliki dan mampu mengoperasikan telepon pintar (*smartphone*).
3. Pernah menggunakan layanan perbankan digital Bank Aceh Syariah (misalnya mobile banking atau internet banking).
4. Berdomisili di Wilayah Kota Banda Aceh

Penentuan jumlah sampel pada penelitian ini menggunakan rumus Cochran. Pemilihan rumus ini didasarkan pada kondisi populasi yang tidak diketahui secara pasti, khususnya jumlah nasabah Bank Aceh Syariah di Kota Banda Aceh yang pernah atau berpotensi mengalami penipuan digital. Rumus Cochran dinilai tepat digunakan untuk menentukan ukuran sampel minimum pada populasi yang tidak teridentifikasi secara jelas jumlahnya.

Rumus Cochran :

$$n = \frac{Z^2 \cdot p \cdot q}{e^2}$$

Keterangan:

n = jumlah sampel

Z = nilai distribusi normal pada tingkat signifikansi 5% (1,96)

p = peluang kejadian (diasumsikan 0,5)

q = 1 – p (0,5)

e = margin of error (tingkat kesalahan) sebesar 5% (0,05)

Penggunaan nilai $p = 0,5$ dan $q = 0,5$ dilakukan karena peneliti tidak memiliki informasi awal mengenai proporsi populasi. Nilai tersebut memberikan ukuran sampel maksimum sehingga hasil penelitian lebih konservatif dan dapat meningkatkan tingkat kepercayaan terhadap hasil penelitian.

Berdasarkan rumus tersebut, maka perhitungan jumlah sampel adalah sebagai berikut:

$$\begin{aligned} n &= \frac{(1,96)^2 \cdot 0,5 \cdot 0,5}{(0,05)^2} \\ &= \frac{3,8416 \cdot 0,25}{0,0025} \\ &= \frac{0,9604}{0,0025} = 384,16 \end{aligned}$$

Hasil perhitungan jumlah sampel diperlukan dalam penelitian ini adalah sebesar 384,16 responden. Karena jumlah sampel harus berupa bilangan bulat, maka angka tersebut dibulatkan menjadi 384 responden.

Selanjutnya, untuk memastikan penyebaran sampel tidak terkonsentrasi pada satu wilayah, peneliti melakukan alokasi sampel ke masing-masing kecamatan menggunakan teknik *Proportionate Stratified Random Sampling*. Pengambilan sampel pada setiap kecamatan dilakukan secara proporsional berdasarkan jumlah penduduk di masing-masing wilayah. Karena jumlah nasabah Bank Aceh Syariah di Kota Banda Aceh tidak diketahui secara pasti, jumlah penduduk berusia di atas 17 tahun digunakan sebagai *proxy* populasi. Data tersebut mengacu pada DPT Pilkada

2024 yang mencakup penduduk yang telah memenuhi syarat usia pemilih. Selanjutnya, data tersebut digunakan sebagai dasar dalam menentukan alokasi sampel pada setiap kecamatan dengan perhitungan sebagai berikut:

Rumus *proportionate stratified random sampling* adalah sebagai berikut:

$$n_i = \frac{N_i}{N} \times n$$

Keterangan:

- n_i = jumlah sampel tiap strata
- N_i = jumlah populasi tiap strata
- N = total populasi
- n = total sampel penelitian (384)

Tabel 3. 1 Sampel Per Kecamatan

No	Kecamatan	Jumlah Populasi	Penjumlahan	Jumlah Sampel
1	Meuraxa	28.153	$(28.153 : 265.310) \times 384 = 40,75$	41
2	Jaya Baru	27.874	$(27.874 : 265.310) \times 384 = 40,34$	40
3	Banda Raya	27.219	$(27.219 : 265.310) \times 384 = 39,39$	39
4	Baiturrahman	32.813	$(32.813 : 265.310) \times 384 = 47,50$	47
5	Lueng Bata	26.274	$(26.274 : 265.310) \times 384 = 38,02$	38
6	Kuta Alam	43.270	$(43.270 : 265.310) \times 384 = 62,63$	63
7	Kuta Raja	15.289	$(15.289 : 265.310) \times 384 = 22,13$	22
8	Syiah Kuala	35.056	$(35.056 : 265.310) \times 384 = 50,74$	51
9	Ulee Kareng	29.362	$(29.362 : 265.310) \times 384 = 42,50$	43
	Total	265.310		384

3.4 Sumber dan Teknik Pengumpulan Data

3.4.1 Sumber Data

Penelitian ini menggunakan data primer sebagai sumber utama. Menurut Sugiyono (2023), data primer merupakan data yang diperoleh secara langsung oleh pengumpul data dari sumber pertama. Dalam penelitian ini, data dikumpulkan langsung dari responden melalui penyebaran kuesioner yang berisi pertanyaan dan pernyataan sesuai dengan kebutuhan penelitian.

3.4.2 Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian ini dilakukan melalui penyebaran kuesioner. Menurut Sugiyono (2023), kuesioner merupakan salah satu metode pengumpulan data yang dilakukan dengan cara memberikan sejumlah pertanyaan atau pernyataan kepada responden untuk dijawab. Metode ini dinilai efektif apabila peneliti telah memahami secara jelas variabel yang akan diukur serta informasi yang dibutuhkan dari responden.

Kuesioner penelitian disebarakan secara daring menggunakan aplikasi Google Forms untuk mempermudah proses distribusi serta meningkatkan efisiensi waktu dan tenaga. Instrumen kuesioner tersebut memuat pertanyaan dan pernyataan yang berkaitan dengan pengaruh literasi digital dan keamanan data pribadi terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

3.5 Definisi dan Operasional Variabel

3.5.1 Variabel Dependen (Y)

Variabel dependen merupakan variabel yang mempengaruhi atau menjadi akibat karena adanya variabel bebas. Dalam penelitian ini variabel dependen yang digunakan yaitu variabel kewaspadaan terhadap penipuan digital (Y). Konsep kewaspadaan terhadap penipuan digital pada penelitian ini diadaptasi dari penelitian Efendi dkk (2025) yang mengacu pada teori Mitnick dan Simon serta disesuaikan dengan konteks perbankan digital. Secara operasional, variabel kewaspadaan terhadap penipuan digital diukur melalui tiga indikator, yaitu: (1) kewaspadaan terhadap berbagai bentuk rekayasa sosial digital, (2) kesadaran terhadap berbagai bentuk rekayasa sosial digital, dan (3) pengetahuan pengguna terhadap berbagai bentuk rekayasa sosial digital. Ketiga indikator tersebut diukur menggunakan skala Likert lima poin, mulai dari sangat tidak setuju hingga sangat setuju.

3.5.2 Variabel Independen (X)

Variabel independen adalah variabel yang berdiri sendiri tanpa dipengaruhi oleh variabel lain, sehingga disebut juga sebagai variabel bebas. Variabel ini berperan sebagai faktor yang mempengaruhi atau penyebab terjadinya perubahan pada variabel terikat (dependent variable), baik secara positif maupun secara negatif. Dalam penelitian ini, variabel independen yang digunakan sebagai berikut:

1. Literasi Digital (X1)

Literasi digital adalah kemampuan nasabah Bank Aceh Syariah dalam mengakses, memahami, mengevaluasi, dan memanfaatkan informasi digital secara efektif serta bertanggung jawab dalam penggunaan layanan perbankan digital. Dalam penelitian ini, literasi digital diukur melalui empat indikator yaitu variabel ini diukur melalui indikator pencarian di internet, navigasi hypertext, evaluasi konten informasi, dan penyusunan pengetahuan (Amri dkk., 2024).

2. Keamanan Data Pribadi (X2)

Keamanan data pribadi merupakan kemampuan individu dalam melindungi informasi pribadi yang digunakan dalam layanan perbankan digital agar terhindar dari akses, penggunaan, perubahan, maupun penyalahgunaan oleh pihak yang tidak berwenang. Dalam penelitian ini, keamanan data pribadi diukur berdasarkan konsep CIA Triad yang terdiri atas kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Kerahasiaan berkaitan dengan kemampuan menjaga data pribadi agar tidak diketahui pihak lain, integritas berkaitan dengan kemampuan menjaga keakuratan dan keutuhan data, sedangkan ketersediaan berkaitan dengan kemampuan memastikan data dapat diakses saat dibutuhkan oleh pihak yang berwenang (Harahap dkk., 2023).

3.5.3 Operasional Variabel

Berdasarkan objek dan metode penelitian, variabel dependen (Y) dalam penelitian ini adalah kewaspadaan terhadap Penipuan Digital. Adapun variabel independen (X) yang dianalisis terdiri dari Literasi Digital (X1) dan Keamanan Data Pribadi (X2). Proses penelitian ini melalui pengumpulan data lapangan menggunakan penyebaran kuesioner yang kemudian dianalisis secara deskriptif untuk menyajikan hasil mengenai pengaruh kedua variabel independen tersebut terhadap variabel dependen.

Tabel 3. 2 Operasionalisasi Variabel

No	Variabel	Indikator	Pernyataan
1	Kewaspadaan terhadap Penipuan Digital (Y)	Kewaspadaan	1. Saya berhati-hati terhadap pesan atau telepon yang mengatasnamakan pihak bank. 2. Saya berhati-hati terhadap tautan dari pihak yang tidak dikenal.
		Kesadaran	1. Saya menyadari bahwa layanan perbankan digital memiliki risiko penipuan. 2. Saya menyadari bahwa pelaku penipuan dapat mengatasnamakan pihak bank untuk memperoleh data pribadi nasabah.
		Pengetahuan berbagai bentuk rekayasa sosial digital	1. Saya mengetahui berbagai modus penipuan digital, seperti <i>phishing</i> dan rekayasa sosial (<i>social engineering</i>). 2. Saya mengetahui bahwa pelaku penipuan digital dapat menyamar sebagai pihak bank atau lembaga keuangan resmi.

No	Variabel	Indikator	Pernyataan
2	Literasi Digital (X1)	Pencarian di Internet (<i>Internet Searching</i>)	1. Saya mampu menggunakan kata kunci yang tepat saat mencari informasi perbankan di internet. 2. Saya mampu menemukan informasi perbankan digital dari sumber yang relevan di internet.
		Navigasi <i>Hypertext</i> (<i>Hypertextual Navigation</i>)	1. Saya mampu menggunakan tautan dan menu pada layanan perbankan digital dengan benar. 2. Saya mampu membedakan situs resmi dan situs palsu layanan perbankan digital.
		Evaluasi Konten Informasi (<i>Content Evaluation</i>)	1. Saya mampu membedakan informasi yang valid dan menyesatkan tentang layanan perbankan di internet. 2. Saya memverifikasi kebenaran informasi dari sumber terpercaya sebelum mempercayai konten yang beredar melalui media digital.
		Penyusunan Pengetahuan (<i>Knowledge Assembly</i>)	1. Saya menggabungkan informasi dari berbagai sumber terpercaya untuk memahami risiko kejahatan digital. 2. Saya memanfaatkan informasi dari berbagai sumber untuk melakukan transaksi perbankan dengan lebih aman.
3	Keamanan Data Pribadi (X2)	Kerahasiaan (<i>Confidentiality</i>)	1. Saya menjaga kerahasiaan PIN, kata sandi, dan kode OTP akun Action Mobile saya. 2. Saya hanya memberikan data pribadi perbankan kepada pihak yang berwenang.
		Integritas (<i>Integrity</i>)	1. Saya memastikan bahwa data pribadi yang saya berikan kepada layanan digital perbankan sudah akurat. 2. Saya bertanggung jawab untuk menjaga kerahasiaan data pribadi yang saya gunakan pada

No	Variabel	Indikator	Pernyataan
			layanan perbankan digital.
		Ketersediaan (Availability)	1. Saya memastikan informasi penting yang berkaitan dengan akun layanan perbankan digital tetap tersedia ketika saya membutuhkannya. 2. Saya memastikan akun layanan perbankan digital saya dapat diakses kembali saat diperlukan melalui prosedur pemulihan akun yang tersedia.

3.6 Skala Pengukuran

Skala pengukuran merupakan suatu kesepakatan yang digunakan sebagai acuan dalam menetapkan rentang interval pada instrumen ukur, sehingga instrumen tersebut dapat menghasilkan data yang bersifat kuantitatif dalam proses pengukuran. Penelitian ini menggunakan skala likert sebagai alat ukur. Skala likert berfungsi untuk mengukur sikap, opini, serta persepsi individu maupun kelompok terhadap suatu fenomena sosial. Adapun pengukuran variabel dilakukan berdasarkan indikator-indikator yang dijadikan landasan dalam penyusunan item pertanyaan atau pernyataan pada instrumen penelitian (Sugiyono, 2023). Skala Likert terdiri dari lima pilihan jawaban berbentuk interval, di mana setiap nilai mencerminkan tingkat atau kategori tertentu. Skala likert yang digunakan dalam penelitian ini ditujukan untuk

mengukur respon subjek ke dalam lima kategori sikap, yaitu Sangat Setuju (SS), Setuju (S), Netral (N), Tidak Setuju (TS), Sangat Tidak Setuju (STS), seperti pada tabel di bawah ini:

Tabel 3. 3 Skala Likert

Keterangan	Skor
Sangat tidak setuju	1
Tidak setuju	2
Netral	3
Setuju	4
Sangat setuju	5

3.7 Metode Analisis Data

Metode analisis data dalam penelitian ini meliputi uji asumsi klasik serta analisis regresi linier berganda yang diolah menggunakan perangkat lunak SPSS (*Statistical Product and Service Solutions*).

3.7.1 Uji Keabsahan Data

3.7.1.1 Uji Validitas

Uji validitas merupakan prosedur yang digunakan untuk menilai sejauh mana suatu instrumen mampu mengukur konstruk yang seharusnya diukur. Menurut Ghazali (2021), uji validitas berfungsi sebagai alat untuk menentukan apakah suatu kuesioner memiliki tingkat keabsahan yang memadai. Suatu kuesioner dinyatakan valid apabila setiap item pertanyaan di dalamnya mampu merepresentasikan variabel yang ingin diukur. Adapun

kriteria yang digunakan dalam menilai validitas adalah sebagai berikut:

- a) Apabila $r \text{ hitung} > r \text{ tabel}$, maka item pernyataan dalam kuesioner dinyatakan valid.
- b) Apabila $r \text{ hitung} < r \text{ tabel}$, maka item pernyataan dalam kuesioner dinyatakan tidak valid.

3.7.1.2 Uji Reliabilitas

Menurut Ghazali (2021), uji reliabilitas merupakan metode yang digunakan untuk menilai sejauh mana suatu kuesioner, sebagai indikator dari variabel atau konstruk, mampu memberikan hasil yang konsisten. Suatu kuesioner dinyatakan reliabel apabila jawaban responden terhadap pernyataan yang diajukan menunjukkan kestabilan atau konsistensi dari waktu ke waktu. Dalam penelitian ini, pengujian reliabilitas dilakukan dengan menggunakan SPSS untuk mengetahui tingkat keterkaitan antar item dalam kuesioner. Suatu konstruk atau variabel dianggap reliabel apabila memiliki nilai Cronbach's Alpha lebih besar dari 0,60.

3.7.2 Uji Asumsi Klasik

3.7.2.1 Uji Normalitas

Uji normalitas bertujuan untuk menilai apakah data pada variabel independen dan dependen dalam model regresi berdistribusi normal atau tidak. Dalam penelitian ini, pengujian normalitas dilakukan dengan menggunakan uji Kolmogorov-

Smirnov (Ghozali, 2021). Adapun dasar pengambilan keputusan dalam uji tersebut adalah sebagai berikut:

- 1) Jika nilai signifikansi $> 0,05$, maka data terdistribusi secara normal.
- 2) Jika nilai signifikansi $< 0,05$ maka data tidak terdistribusi dengan normal.

3.7.2.2 Uji Multikolinearitas

Menurut Ghozali (2021) uji multikolinearitas merupakan prosedur yang digunakan untuk mengidentifikasi ada atau tidaknya hubungan (korelasi) antar variabel independen dalam suatu model regresi. Pengujian ini bertujuan untuk mengetahui apakah terdapat hubungan linear yang kuat di antara variabel bebas yang berpotensi memengaruhi ketepatan model. Uji multikolinearitas umumnya dilakukan dengan melihat nilai *Variance Inflation Factor* (VIF) dan *tolerance*, yang menunjukkan sejauh mana suatu variabel independen dapat dijelaskan oleh variabel independen lainnya. Multikolinearitas dapat diindikasikan apabila nilai tolerance kurang dari 0,10 atau nilai VIF melebihi 10. Sebaliknya, jika seluruh nilai VIF berada di bawah 10, maka dapat disimpulkan bahwa tidak terdapat masalah multikolinearitas yang serius, sehingga model dinyatakan memenuhi asumsi multikolinearitas.

3.7.2.3 Uji Heteroskedastisitas

Uji heteroskedastisitas bertujuan untuk menilai apakah dalam model regresi terdapat ketidaksamaan varians residual antara

satu pengamatan dengan pengamatan lainnya. Jika varians residual bersifat konstan, kondisi tersebut disebut homoskedastisitas, sedangkan apabila variansnya berbeda maka disebut heteroskedastisitas (Ghozali, 2021). Dalam penelitian ini, uji yang digunakan adalah metode scatterplot. Dimana sumbu horizontal menggambarkan Predicted Standardized sedangkan sumbu vertikal menggambarkan Residual Studentize. Adapun dasar dari pengambilan keputusan dalam uji ini yakni sebagai berikut:

- 1) Jika plot menyebar secara acak diatas maupun dibawah angka nol pada sumbu Regression Studentized Residual maka tidak terdapat gejala heteroskedastisitas.
- 2) Jika plot membentuk pola tertentu maka terdapat gejala heteroskedastisitas.

3.8 Uji Regresi Linear Berganda

Uji regresi linear berganda dalam penelitian ini digunakan untuk menganalisis hubungan kausal antara dua atau lebih variabel independen dengan satu variabel dependen (Ghozali, 2021). Melalui pengujian ini, dapat diketahui pengaruh variabel Literasi Digital (X1) dan Keamanan Data Pribadi (X2) terhadap variabel Penipuan Digital (Y).

Adapun persamaan yang digunakan dalam analisis regresi linear berganda adalah sebagai berikut :

$$Y = a + b_1X_1 + b_2X_2 + e$$

Keterangan:

Y : Kewaspadaan terhadap Penipuan Digital

a : Konstanta dari persamaan regresi

b1, b2 : Koefisien regresi variabel independen

X1 : Literasi Digital

X2 : Keamanan Data Pribadi

e : *Standard error*

3.9 Uji Hipotesis

3.9.1 Uji T (Uji Parsial)

Uji t digunakan untuk mengetahui sejauh mana pengaruh variabel independen dalam menjelaskan variasi pada variabel dependen, serta untuk menilai pengaruh masing-masing variabel bebas secara individual terhadap variabel terikat (Ghozali, 2021). Pengambilan keputusan dilakukan dengan membandingkan nilai t hitung dan t tabel, di mana jika t hitung lebih besar dari t tabel, maka variabel independen secara parsial berpengaruh terhadap variabel dependen. Dengan demikian, uji t bertujuan untuk menguji signifikansi pengaruh setiap variabel independen secara individu terhadap variabel terikat pada tingkat signifikansi tertentu, dengan asumsi variabel bebas lainnya dalam kondisi konstan.

1. Jika nilai signifikan lebih besar dari 0,05 atau $t_{hitung} < t_{tabel}$ maka H_0 diterima dan H_a ditolak, atau variabel independen tidak berpengaruh signifikan terhadap variabel dependen.

2. Jika nilai signifikan lebih kecil dari 0,05 atau $t_{hitung} > t_{tabel}$ maka H_a diterima dan H_0 ditolak, atau variabel independen berpengaruh signifikan terhadap variabel dependen.

3.9.2 Uji F (Uji Simultan)

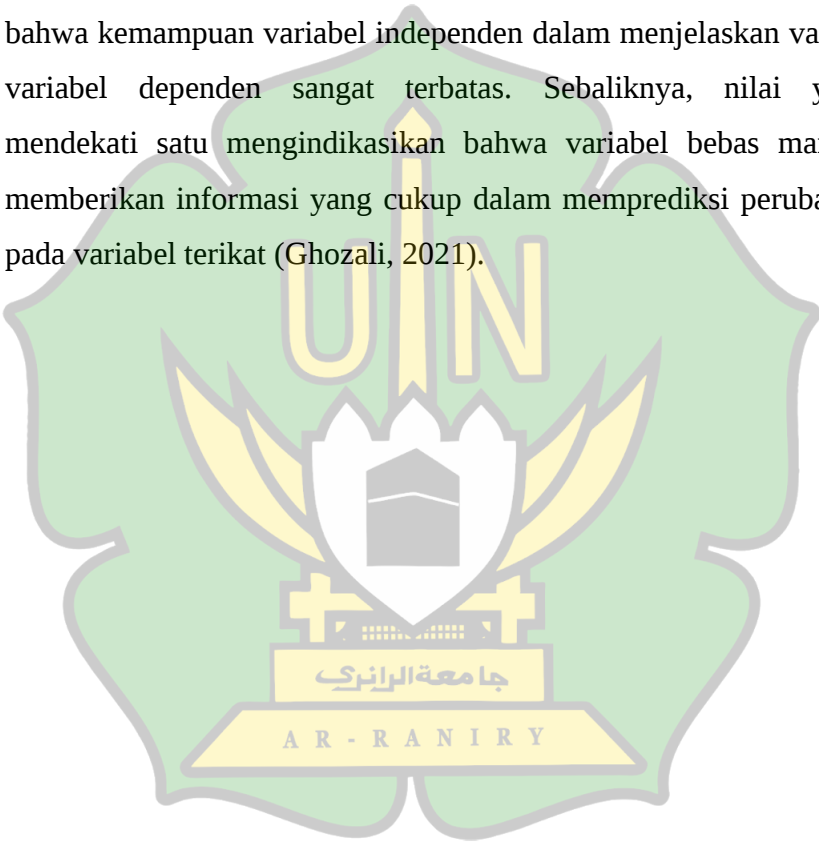
Uji F atau uji simultan digunakan untuk mengetahui apakah seluruh variabel independen dalam model regresi secara bersama-sama memiliki pengaruh terhadap variabel dependen (Ghozali, 2021). Dalam penelitian ini, pengujian hipotesis secara simultan bertujuan untuk menganalisis besarnya pengaruh literasi digital (X1) dan keamanan data pribadi (X2) terhadap kewaspadaan terhadap penipuan digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

Adapun kriteria dasar dalam pengambilan keputusan pada pengujian hipotesis ini adalah sebagai berikut :

1. Jika nilai signifikan lebih kecil dari 0,05 atau $F_{hitung} > F_{tabel}$ maka H_0 ditolak dan H_a diterima, yang artinya semua variabel independen mempunyai pengaruh secara bersama-sama terhadap variabel dependen.
2. Jika nilai signifikan lebih besar dari 0,05 atau $F_{hitung} < F_{tabel}$ maka H_0 diterima dan H_a ditolak, yang artinya semua variabel independen tidak mempunyai pengaruh secara bersama-sama terhadap variabel dependen.

3.9.3 Uji Koefisien Determinasi (R^2)

Uji koefisien determinasi digunakan untuk menilai sejauh mana variabel independen mampu menjelaskan variasi pada variabel dependen. Nilai koefisien determinasi berada pada rentang 0 hingga 1. Apabila nilainya rendah, hal tersebut enunjukkan bahwa kemampuan variabel independen dalam menjelaskan variasi variabel dependen sangat terbatas. Sebaliknya, nilai yang mendekati satu mengindikasikan bahwa variabel bebas mampu memberikan informasi yang cukup dalam memprediksi perubahan pada variabel terikat (Ghozali, 2021).



BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Gambaran Umum Lokasi Penelitian

Kota Banda Aceh merupakan Ibu Kota Provinsi Aceh sekaligus pusat pemerintahan, perekonomian, dan aktivitas keuangan di wilayah tersebut. Secara geografis, Kota Banda Aceh terletak di ujung paling barat Pulau Sumatera dan berbatasan dengan Selat Malaka di sebelah utara, Kabupaten Aceh Besar di sebelah timur dan barat, serta Samudera Hindia di sebelah barat. Wilayah ini memiliki ketinggian rata-rata sekitar 0,80 meter di atas permukaan laut.

Secara administratif, Kota Banda Aceh terbagi ke dalam 9 (sembilan) kecamatan yang merupakan unit pemerintahan di tingkat kota, yaitu Kecamatan Meuraxa, Jaya Baru, Banda Raya, Baiturrahman, Lueng Bata, Kuta Alam, Kuta Raja, Syiah Kuala, dan Ulee Kareng. Posisi Kota Banda Aceh sebagai pusat aktivitas ekonomi dan keuangan menjadikannya lokasi yang representatif untuk mengkaji perilaku nasabah dalam penggunaan layanan perbankan syariah berbasis digital, termasuk kewaspadaan nasabah terhadap berbagai bentuk penipuan digital. Adapun luas wilayah dan jumlah penduduk masing-masing kecamatan di Kota Banda Aceh dapat dilihat pada tabel berikut.

Tabel 4. 1 Luas Wilayah dan Jumlah Penduduk Masing-Masing Kecamatan di Kota Banda Aceh

No	Kecamatan	Luas (KM ²)	Jumlah Penduduk
1	Meuraxa	7,26	28.153
2	Jaya Baru	3,78	27.874
3	Banda Raya	4,79	27.219
4	Baiturrahman	4,54	32.813
5	Lueng Bata	5,34	26.274
6	Kuta Alam	10,21	43.270
7	Kuta Raja	5,21	15.289
8	Syiah Kuala	14,24	35.056
9	Ulee Kareng	6,15	29.362
	Jumlah	61,52	265.310

4.2 Hasil Penelitian

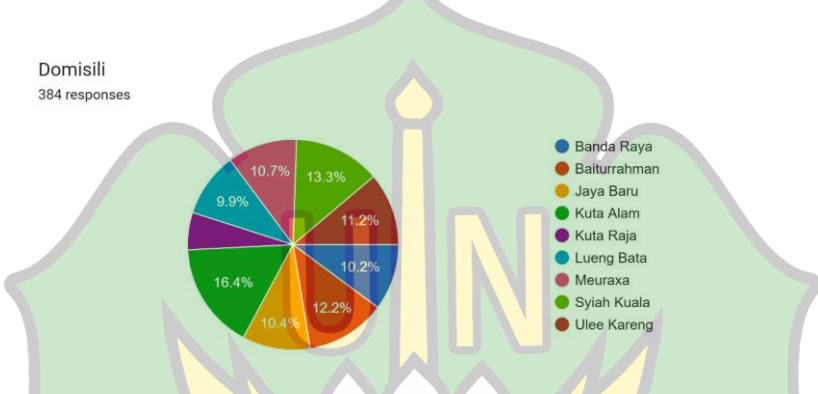
Hasil penelitian ini diperoleh melalui penyebaran kuesioner kepada 384 responden yang telah memenuhi kriteria yang ditetapkan, yaitu merupakan nasabah Bank Aceh Syariah, memiliki dan mampu mengoperasikan telepon pintar (smartphone), pernah menggunakan layanan perbankan digital Bank Aceh Syariah, serta berdomisili di Kota Banda Aceh. Kuesioner disebarikan secara daring melalui Google Forms dengan memanfaatkan berbagai akun media sosial dan grup percakapan, di samping penyebaran secara langsung kepada beberapa responden yang memenuhi kriteria. Adapun hasil penelitian ini dipaparkan berdasarkan karakteristik responden serta hasil pengujian data sebagai berikut.

4.2.1 Karakteristik Responden

1. Karakteristik Responden Berdasarkan Domisili

Adapun karakteristik responden penelitian berdasarkan domisili dapat dilihat pada gambar 4.1 berikut:

Gambar 4. 1 Diagram Karakteristik Responden Berdasarkan Domisili



Sumber: data primer diolah (2026)

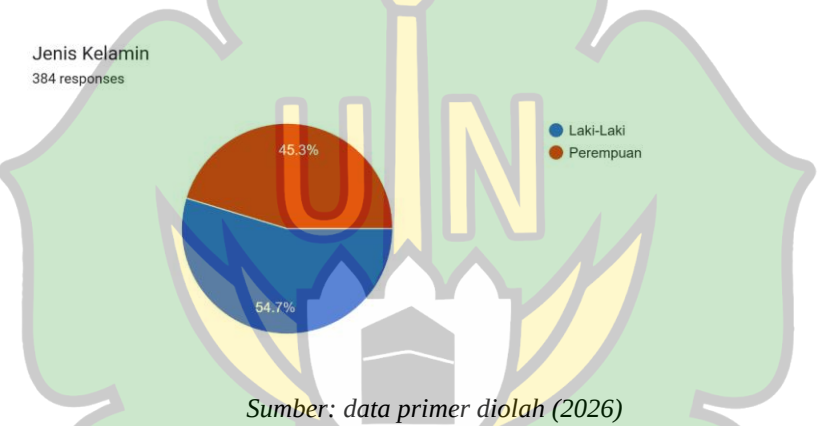
Berdasarkan gambar 4.1, dapat dilihat bahwa responden tersebar secara proporsional di 9 kecamatan di Kota Banda Aceh. Responden paling banyak berdomisili di Kecamatan Kuta Alam yaitu sebanyak 63 responden (16,4%), diikuti Kecamatan Syiah Kuala sebanyak 51 responden (13,3%), Kecamatan Baiturrahman sebanyak 47 responden (12,2%), Kecamatan Ulee Kareng sebanyak 43 responden (11,2%), Kecamatan Meuraxa sebanyak 41 responden (10,7%), Kecamatan Jaya Baru sebanyak 40 responden (10,4%), Kecamatan Banda Raya sebanyak 39 responden (10,2%), Kecamatan Lueng Bata sebanyak 38 responden (9,9%), dan yang paling sedikit adalah Kecamatan Kuta Raja sebanyak 22 responden (5,7%). Sebaran ini sejalan dengan proporsi jumlah penduduk pada

masing-masing kecamatan karena pengambilan sampel dilakukan dengan teknik proportionate stratified random sampling.

2. Karakteristik Responden Berdasarkan Jenis Kelamin

Adapun karakteristik responden penelitian berdasarkan jenis kelamin dapat dilihat pada gambar 4.2 sebagai berikut:

Gambar 4. 2 Diagram Karakteristik Responden Berdasarkan Jenis Kelamin



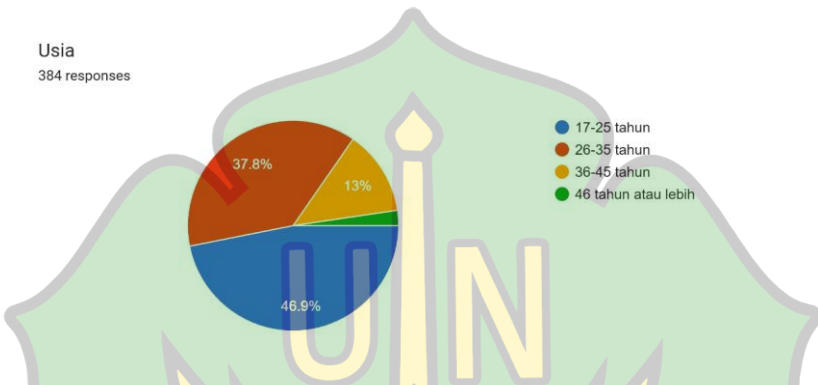
Sumber: data primer diolah (2026)

Berdasarkan gambar 4.2, dapat dilihat bahwa dari 384 responden penelitian, mayoritas responden berjenis kelamin laki-laki yaitu sebanyak 210 responden (54,7%), sedangkan responden berjenis kelamin perempuan berjumlah 174 responden (45,3%). Hal ini menunjukkan bahwa nasabah Bank Aceh Syariah yang menjadi responden dalam penelitian ini relatif seimbang antara laki-laki dan perempuan, dengan proporsi laki-laki sedikit lebih dominan.

3. Karakteristik Responden Berdasarkan Usia

Adapun karakteristik responden penelitian berdasarkan kelompok usia dapat dilihat pada gambar 4.3 sebagai berikut:

Gambar 4. 3 Diagram Karakteristik Responden Berdasarkan Usia



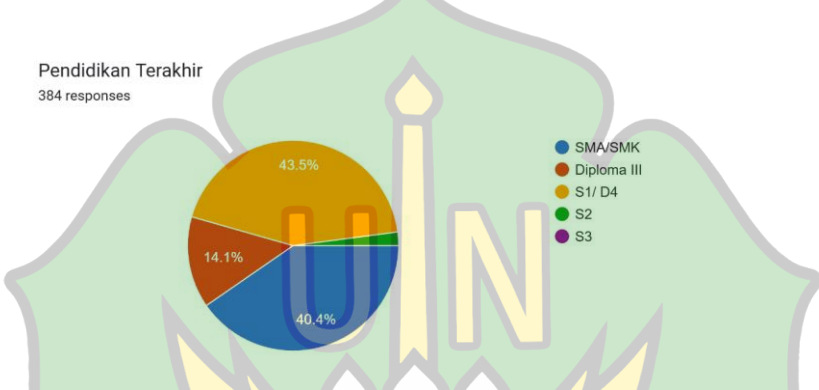
Sumber: data primer diolah (2026)

Berdasarkan gambar 4.3, dari total 384 responden, mayoritas berada pada rentang usia 17-25 tahun yaitu sebanyak 180 responden (46,9%), diikuti rentang usia 26-35 tahun sebanyak 145 responden (37,8%), rentang usia 36-45 tahun sebanyak 50 responden (13,0%), dan responden berusia 46 tahun atau lebih memiliki jumlah paling sedikit yaitu 9 responden (2,3%). Hal ini menunjukkan bahwa responden dalam penelitian ini didominasi oleh generasi muda yang secara umum lebih terbiasa dengan penggunaan layanan perbankan berbasis digital, namun pada saat yang sama juga rentan menjadi sasaran penipuan digital apabila tidak diimbangi dengan literasi digital dan kesadaran keamanan data yang memadai.

4. Karakteristik Responden Berdasarkan Pendidikan Terakhir

Adapun karakteristik responden penelitian berdasarkan pendidikan terakhir dapat dilihat pada gambar 4.4 sebagai berikut:

Gambar 4. 4 Diagram Karakteristik Responden Berdasarkan Pendidikan Terakhir



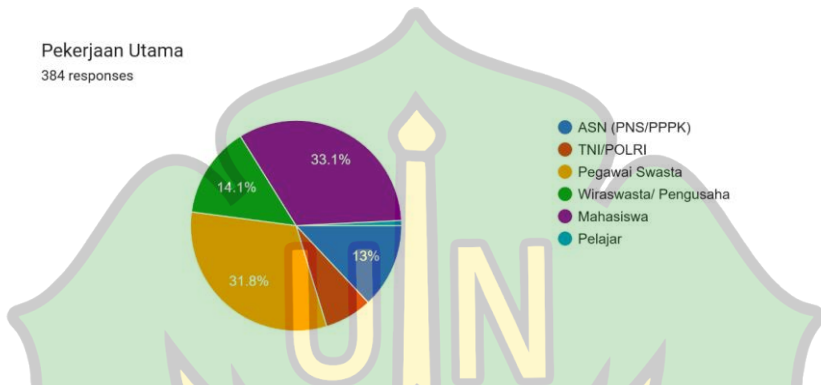
Sumber: data primer diolah (2026)

Berdasarkan gambar 4.4, karakteristik responden berdasarkan pendidikan terakhir menunjukkan variasi yang cukup beragam. Dari 384 responden, mayoritas memiliki pendidikan terakhir S1/D4 yaitu sebanyak 167 responden (43,5%), diikuti pendidikan SMA sebanyak 155 responden (40,4%), pendidikan Diploma III sebanyak 54 responden (14,1%), dan pendidikan S2 sebanyak 8 responden (2,1%), sedangkan tidak terdapat responden dengan pendidikan S3. Hal ini menunjukkan bahwa mayoritas responden memiliki latar belakang pendidikan menengah hingga tinggi, sehingga secara umum memiliki kemampuan literasi digital yang cukup untuk memahami instrumen penelitian dan risiko penipuan digital.

5. Karakteristik Responden Berdasarkan Pekerjaan

Adapun karakteristik responden penelitian berdasarkan kelompok pekerjaan dapat dilihat pada gambar 4.5 sebagai berikut:

Gambar 4. 5 Diagram Karakteristik Responden Berdasarkan Pekerjaan



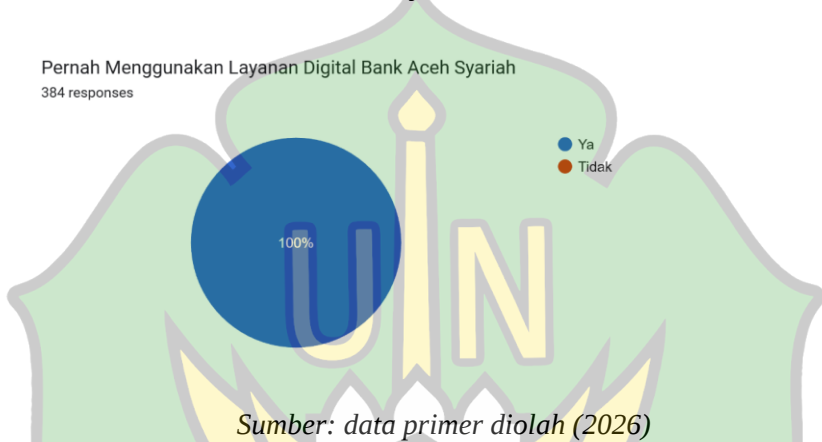
Sumber: data primer diolah (2026)

Berdasarkan gambar 4.5, dapat dilihat bahwa responden paling banyak berprofesi sebagai mahasiswa yaitu sebanyak 127 responden (33,1%), diikuti pegawai swasta sebanyak 122 responden (31,8%), ASN sebanyak 50 responden (13,0%), wiraswasta sebanyak 54 responden (14,1%), TNI/Polri sebanyak 28 responden (7,3%), dan pelajar sebanyak 3 responden (0,8%). Data ini menunjukkan bahwa responden dalam penelitian ini didominasi oleh mahasiswa dan pegawai swasta, yang merupakan kelompok masyarakat yang aktif menggunakan layanan perbankan digital dalam aktivitas sehari-hari.

6. Karakteristik Responden Berdasarkan Pengalaman Menggunakan Layanan Digital Bank Aceh Syariah

Adapun karakteristik responden penelitian berdasarkan pengalaman menggunakan layanan digital Bank Aceh Syariah dapat dilihat pada gambar 4.6 sebagai berikut:

Gambar 4. 6 Diagram Karakteristik Responden Berdasarkan Pengalaman Menggunakan Layanan Digital Bank Aceh Syariah



Berdasarkan gambar 4.6, dapat diketahui bahwa seluruh responden yaitu sebanyak 384 responden (100%) menyatakan pernah menggunakan layanan digital Bank Aceh Syariah, seperti mobile banking dan/atau ATM. Hal ini sesuai dengan kriteria sampel yang telah ditetapkan dalam penelitian ini, sehingga seluruh responden dapat dinilai memiliki pengalaman yang relevan untuk menilai literasi digital, keamanan data pribadi, serta potensi kewaspadaan terhadap penipuan digital yang dihadapi selama menggunakan layanan tersebut.

4.3 Tanggapan Responden Terhadap Variabel Penelitian

Berikut ini disajikan tanggapan responden terhadap setiap item pernyataan pada kuesioner untuk masing-masing variabel

penelitian, yaitu Literasi Digital (X1), Keamanan Data Pribadi (X2), dan kewaspadaan terhadap Penipuan Digital (Y).

4.3.1 Tanggapan Responden Terhadap Variabel Literasi Digital (X1)

Adapun tanggapan responden terhadap variabel Literasi Digital (X1) dapat dilihat pada tabel 4.2 berikut:

Tabel 4. 2 Tanggapan Responden Terhadap Variabel Literasi Digital (X1)

No.	Pernyataan	Skala Jawaban	Frekuensi Jawaban X Nilai Skala = Hasil	Rata-Rata
1	Saya mampu menggunakan kata kunci yang tepat saat mencari informasi perbankan di internet	STS	$1 \times 1 = 1$	
		TS	$10 \times 2 = 20$	
		N	$15 \times 3 = 45$	
		S	$201 \times 4 = 804$	
		SS	$157 \times 5 = 785$	
		Total = 1.655 : 384		4,31
		$1.655 : (5 \times 384) \times 100\%$		86,20
2	Saya mampu menemukan informasi perbankan digital dari sumber yang relevan di internet	STS	$4 \times 1 = 4$	
		TS	$25 \times 2 = 50$	
		N	$52 \times 3 = 156$	
		S	$160 \times 4 = 640$	
		SS	$143 \times 5 = 715$	
		Total = 1.565 : 384		4,08
		$1.565 : (5 \times 384) \times 100\%$		81,51
3	Saya mampu menggunakan tautan dan menu pada layanan perbankan digital dengan benar	STS	$7 \times 1 = 7$	
		TS	$9 \times 2 = 18$	
		N	$74 \times 3 = 222$	
		S	$134 \times 4 = 536$	
		SS	$160 \times 5 = 800$	
		Total = 1.583 : 384		4,12
		$1.583 : (5 \times 384) \times 100\%$		82,45
4	Saya mampu membedakan situs resmi dan situs palsu layanan perbankan digital	STS	$14 \times 1 = 14$	
		TS	$37 \times 2 = 74$	
		N	$87 \times 3 = 261$	
		S	$108 \times 4 = 432$	
		SS	$138 \times 5 = 690$	

		Total = 1.471 : 384		3,83
		1.471 : (5 x 384) x 100%		76,61
5	Saya mampu membedakan informasi yang valid dan menyesatkan tentang layanan perbankan di internet	STS	4 x 1 = 4	
		TS	23 x 2 = 46	
		N	65 x 3 = 195	
		S	118 x 4 = 472	
		SS	174 x 5 = 870	
		Total = 1.587 : 384		4,13
		1.587 : (5 x 384) x 100%		82,66
6	Saya memverifikasi kebenaran informasi dari sumber terpercaya sebelum mempercayai konten yang beredar melalui media digital	STS	1 x 1 = 1	
		TS	13 x 2 = 26	
		N	53 x 3 = 159	
		S	187 x 4 = 748	
		SS	130 x 5 = 650	
		Total = 1.584 : 384		4,12
		1.584 : (5 x 384) x 100%		82,50
7	Saya menggabungkan informasi dari berbagai sumber terpercaya untuk memahami risiko kejahatan digital	STS	12 x 1 = 12	
		TS	25 x 2 = 50	
		N	44 x 3 = 132	
		S	150 x 4 = 600	
		SS	153 x 5 = 765	
		Total = 1.559 : 384		4,06
		1.559 : (5 x 384) x 100%		81,20
8	Saya memanfaatkan informasi dari berbagai sumber untuk melakukan transaksi perbankan dengan lebih aman	STS	4 x 1 = 4	
		TS	11 x 2 = 22	
		N	46 x 3 = 138	
		S	178 x 4 = 712	
		SS	145 x 5 = 725	
		Total = 1.601 : 384		4,17
		1.601 : (5 x 384) x 100%		83,39

Sumber: Data primer diolah (2026)

Tabel 4.2 menunjukkan bahwa tanggapan responden terhadap seluruh item pernyataan pada variabel Literasi Digital berada pada kategori tinggi. Item nomor 1, yaitu “Saya mampu menggunakan kata kunci yang tepat saat mencari informasi perbankan di internet”, memperoleh nilai rata-rata tertinggi sebesar 4,31 atau 86,20%. Item nomor 2 mengenai kemampuan menemukan informasi perbankan digital dari sumber yang relevan

memperoleh nilai rata-rata 4,08 atau 81,51%. Item nomor 3 mengenai kemampuan menggunakan tautan dan menu pada layanan perbankan digital dengan benar memperoleh nilai rata-rata 4,12 atau 82,45%. Item nomor 5 mengenai kemampuan membedakan informasi yang valid dan menyesatkan tentang layanan perbankan di internet memperoleh nilai rata-rata 4,13 atau 82,66%. Item nomor 6 mengenai verifikasi kebenaran informasi dari sumber terpercaya sebelum mempercayai konten yang beredar di media digital memperoleh nilai rata-rata 4,12 atau 82,50%. Item nomor 7 mengenai penggabungan informasi dari berbagai sumber terpercaya untuk memahami risiko kejahatan digital memperoleh nilai rata-rata 4,06 atau 81,20%. Item nomor 8 mengenai pemanfaatan informasi dari berbagai sumber untuk melakukan transaksi perbankan dengan lebih aman memperoleh nilai rata-rata 4,17 atau 83,39%. Adapun nilai terendah terdapat pada item nomor 4, yaitu “Saya mampu membedakan situs resmi dan situs palsu layanan perbankan digital”, dengan nilai rata-rata 3,83 atau 76,61%.

4.3.2 Tanggapan Responden Terhadap Variabel Keamanan Data Pribadi (X2)

Adapun tanggapan responden terhadap variabel Keamanan Data Pribadi (X2) dapat dilihat pada tabel 4.3 berikut:

Tabel 4. 3 Tanggapan Responden Terhadap Variabel Keamanan Data Pribadi (X2)

No.	Pernyataan	Skala Jawaban	Frekuensi Jawaban X Nilai Skala = Hasil	Rata-Rata
1	Saya menjaga kerahasiaan PIN, kata sandi, dan kode OTP akun Action Mobile saya	STS	$3 \times 1 = 3$	
		TS	$8 \times 2 = 16$	
		N	$35 \times 3 = 105$	
		S	$176 \times 4 = 704$	
		SS	$162 \times 5 = 810$	
		Total = 1.638 : 384		4,27
		$1.638 : (5 \times 384) \times 100\%$		85,31
2	Saya hanya memberikan data pribadi perbankan kepada pihak yang berwenang	STS	$2 \times 1 = 2$	
		TS	$10 \times 2 = 20$	
		N	$86 \times 3 = 258$	
		S	$137 \times 4 = 548$	
		SS	$149 \times 5 = 745$	
		Total = 1.573 : 384		4,10
		$1.573 : (5 \times 384) \times 100\%$		81,93
3	Saya memastikan bahwa data pribadi yang saya berikan kepada layanan digital perbankan sudah akurat	STS	$5 \times 1 = 5$	
		TS	$7 \times 2 = 14$	
		N	$68 \times 3 = 204$	
		S	$150 \times 4 = 600$	
		SS	$154 \times 5 = 770$	
		Total = 1.593 : 384		4,15
		$1.593 : (5 \times 384) \times 100\%$		82,97
4	Saya bertanggung jawab untuk menjaga kerahasiaan data pribadi yang saya gunakan pada layanan perbankan digital	STS	$19 \times 1 = 19$	
		TS	$36 \times 2 = 72$	
		N	$57 \times 3 = 171$	
		S	$129 \times 4 = 516$	
		SS	$143 \times 5 = 715$	
		Total = 1.493 : 384		3,89
		$1.493 : (5 \times 384) \times 100\%$		77,76
5	Saya memastikan informasi penting yang berkaitan dengan akun layanan perbankan digital tetap tersedia ketika saya membutuhkannya	STS	$7 \times 1 = 7$	
		TS	$28 \times 2 = 56$	
		N	$60 \times 3 = 180$	
		S	$127 \times 4 = 508$	
		SS	$162 \times 5 = 810$	
		Total = 1.561 : 384		4,07
		$1.561 : (5 \times 384) \times 100\%$		81,30
6	Saya memastikan akun layanan perbankan	STS	$5 \times 1 = 5$	
		TS	$9 \times 2 = 18$	

digital saya dapat diakses kembali saat diperlukan melalui prosedur pemulihan akun yang tersedia	N	$58 \times 3 = 174$	
	S	$202 \times 4 = 808$	
	SS	$110 \times 5 = 550$	
	Total = $1.555 : 384$		4,05
	$1.555 : (5 \times 384) \times 100\%$		80,99

Sumber: Data primer diolah (2026)

Tabel 4.3 menunjukkan bahwa tanggapan responden terhadap seluruh item pernyataan pada variabel Keamanan Data Pribadi berada pada kategori tinggi. Item nomor 1, yaitu “Saya menjaga kerahasiaan PIN, kata sandi, dan kode OTP akun Action Mobile saya”, memperoleh nilai rata-rata tertinggi sebesar 4,27 atau 85,31%. Item nomor 2 mengenai pemberian data pribadi perbankan hanya kepada pihak yang berwenang memperoleh nilai rata-rata 4,10 atau 81,93%. Item nomor 3 mengenai memastikan data pribadi yang diberikan kepada layanan digital perbankan sudah akurat memperoleh nilai rata-rata 4,15 atau 82,97%. Item nomor 5 mengenai memastikan informasi penting terkait akun layanan perbankan digital tetap tersedia saat dibutuhkan memperoleh nilai rata-rata 4,07 atau 81,30%. Item nomor 6 mengenai memastikan akun layanan perbankan digital dapat diakses kembali melalui prosedur pemulihan akun memperoleh nilai rata-rata 4,05 atau 80,99%. Adapun nilai terendah terdapat pada item nomor 4, yaitu “Saya bertanggung jawab untuk menjaga kerahasiaan data pribadi yang saya gunakan pada layanan perbankan digital”, dengan nilai rata-rata 3,89 atau 77,76%.

4.3.3 Tanggapan Responden Terhadap Variabel Kewaspadaan terhadap Penipuan Digital (Y)

Adapun tanggapan responden terhadap variabel kewaspadaan terhadap Penipuan Digital (Y) dapat dilihat pada tabel 4.4 berikut:

Tabel 4. 4 Tanggapan Responden Terhadap Variabel kewaspadaan terhadap Penipuan Digital (Y)

No.	Pernyataan	Skala Jawaban	Frekuensi Jawaban X Nilai Skala = Hasil	Rata-Rata
1	Saya berhati-hati terhadap pesan atau telepon yang mengatasnamakan pihak bank	STS	$5 \times 1 = 5$	
		TS	$6 \times 2 = 12$	
		N	$39 \times 3 = 117$	
		S	$186 \times 4 = 744$	
		SS	$148 \times 5 = 740$	
		Total = 1.618 : 384		4,21
		$1.618 : (5 \times 384) \times 100\%$		84,27
2	Saya berhati-hati terhadap tautan dari pihak yang tidak dikenal	STS	$5 \times 1 = 5$	
		TS	$11 \times 2 = 22$	
		N	$67 \times 3 = 201$	
		S	$143 \times 4 = 572$	
		SS	$158 \times 5 = 790$	
		Total = 1.590 : 384		4,14
		$1.590 : (5 \times 384) \times 100\%$		82,81
3	Saya menyadari bahwa layanan perbankan digital memiliki risiko penipuan	STS	$4 \times 1 = 4$	
		TS	$7 \times 2 = 14$	
		N	$56 \times 3 = 168$	
		S	$172 \times 4 = 688$	
		SS	$145 \times 5 = 725$	
		Total = 1.599 : 384		4,16
		$1.599 : (5 \times 384) \times 100\%$		83,28
4	Saya menyadari bahwa pelaku penipuan dapat mengatasnamakan pihak bank untuk memperoleh data pribadi nasabah	STS	$21 \times 1 = 21$	
		TS	$30 \times 2 = 60$	
		N	$61 \times 3 = 183$	
		S	$128 \times 4 = 512$	
		SS	$144 \times 5 = 720$	
		Total = 1.496 : 384		3,90

		$1.496 : (5 \times 384) \times 100\%$		77,92
5	Saya mengetahui berbagai modus penipuan digital, seperti phishing dan rekayasa sosial (social engineering)	STS	$7 \times 1 = 7$	
		TS	$30 \times 2 = 60$	
		N	$48 \times 3 = 144$	
		S	$129 \times 4 = 516$	
		SS	$170 \times 5 = 850$	
		Total = $1.577 : 384$		4,11
		$1.577 : (5 \times 384) \times 100\%$		82,14
6	Saya mengetahui ciri-ciri pesan, telepon, atau situs palsu, yang mengatasnamakan pihak bank.	STS	$9 \times 1 = 9$	
		TS	$16 \times 2 = 32$	
		N	$43 \times 3 = 129$	
		S	$188 \times 4 = 752$	
		SS	$128 \times 5 = 640$	
		Total = $1.562 : 384$		4,07
		$1.562 : (5 \times 384) \times 100\%$		81,35

Sumber: Data primer diolah (2026)

Tabel 4.4 menunjukkan bahwa tanggapan responden terhadap seluruh item pernyataan pada variabel kewaspadaan terhadap Penipuan Digital berada pada kategori tinggi. Item nomor 1, yaitu “Saya berhati-hati terhadap pesan atau telepon yang mengatasnamakan pihak bank”, memperoleh nilai rata-rata tertinggi sebesar 4,21 atau 84,27%. Item nomor 2 mengenai kehati-hatian terhadap tautan dari pihak yang tidak dikenal memperoleh nilai rata-rata 4,14 atau 82,81%. Item nomor 3 mengenai kesadaran bahwa layanan perbankan digital memiliki risiko penipuan memperoleh nilai rata-rata 4,16 atau 83,28%. Item nomor 5 mengenai pengetahuan tentang berbagai modus penipuan digital, seperti phishing dan rekayasa sosial, memperoleh nilai rata-rata 4,11 atau 82,14%. Item nomor 6 mengenai pengetahuan tentang ciri-ciri pesan, telepon, atau situs palsu yang mengatasnamakan pihak bank memperoleh nilai rata-rata 4,07 atau 81,35%. Adapun

nilai terendah terdapat pada item nomor 4, yaitu “Saya menyadari bahwa pelaku penipuan dapat mengatasnamakan pihak bank untuk memperoleh data pribadi nasabah”, dengan nilai rata-rata 3,90 atau 77,92%.

4.4 Hasil Uji Validitas dan Reliabilitas

4.4.1 Uji Validitas

Uji validitas dilakukan untuk memastikan bahwa setiap item pernyataan dalam kuesioner yang telah disebarakan kepada responden benar-benar mampu mengukur variabel yang diteliti. Pengujian dilakukan dengan membandingkan nilai r hitung (Pearson Correlation) masing-masing item terhadap skor total variabel dengan nilai r tabel. Nilai r tabel diperoleh melalui derajat kebebasan (df) = $n-2$ = $384-2$ = 382 pada taraf signifikansi 5%, yaitu sebesar 0,100. Apabila r hitung $>$ r tabel, maka item pernyataan dinyatakan valid. Adapun hasil pengujian validitas adalah sebagai berikut:

Tabel 4. 5 Hasil Uji Validitas

Item Pernyataan	r hitung	r tabel	Keterangan
X1.1	0,420	0,100	Valid
X1.2	0,666	0,100	Valid
X1.3	0,624	0,100	Valid
X1.4	0,639	0,100	Valid
X1.5	0,480	0,100	Valid
X1.6	0,480	0,100	Valid
X1.7	0,629	0,100	Valid

X1.8	0,545	0,100	Valid
X2.1	0,487	0,100	Valid
X2.2	0,594	0,100	Valid
X2.3	0,535	0,100	Valid
X2.4	0,768	0,100	Valid
X2.5	0,654	0,100	Valid
X2.6	0,554	0,100	Valid
Y.1	0,527	0,100	Valid
Y.2	0,627	0,100	Valid
Y.3	0,486	0,100	Valid
Y.4	0,697	0,100	Valid
Y.5	0,697	0,100	Valid
Y.6	0,622	0,100	Valid

Sumber: Hasil olah data SPSS (2026)

Berdasarkan tabel 4.5, dapat diketahui bahwa seluruh item pernyataan pada variabel Literasi Digital (X1), Keamanan Data Pribadi (X2), maupun kewaspadaan terhadap Penipuan Digital (Y) memiliki nilai r hitung lebih besar dari nilai r tabel sebesar 0,100. Dengan demikian, seluruh item pernyataan dalam kuesioner penelitian ini dinyatakan valid dan layak digunakan sebagai instrumen pengumpulan data.

4.4.2 Uji Reliabilitas

Uji reliabilitas dilakukan terhadap item-item pernyataan yang sebelumnya telah dinyatakan valid, dengan tujuan untuk mengetahui konsistensi jawaban responden terhadap instrumen penelitian. Suatu variabel dinyatakan reliabel apabila nilai

Cronbach's Alpha lebih besar dari 0,60. Adapun hasil pengujian reliabilitas adalah sebagai berikut:

Tabel 4. 6 Hasil Uji Reliabilitas

Variabel	Jumlah Item	Cronbach's Alpha	Nilai Minimal	Keterangan
Literasi Digital (X1)	8	0,693	0,60	Reliabel
Keamanan Data Pribadi (X2)	6	0,654	0,60	Reliabel
Kewaspadaan terhadap Penipuan Digital (Y)	6	0,668	0,60	Reliabel

Sumber: Hasil olah data SPSS (2026)

Berdasarkan tabel 4.6, diketahui bahwa nilai Cronbach's Alpha pada variabel Literasi Digital (X1) sebesar 0,693, variabel Keamanan Data Pribadi (X2) sebesar 0,654, dan variabel kewaspadaan terhadap Penipuan Digital (Y) sebesar 0,668. Nilai tersebut menunjukkan bahwa seluruh variabel memiliki koefisien Cronbach's Alpha lebih besar dari 0,60, sehingga dapat disimpulkan bahwa seluruh instrumen dalam penelitian ini reliabel atau konsisten digunakan untuk mengukur variabel penelitian.

4.5 Hasil Uji Asumsi Klasik

4.5.1 Uji Normalitas

Uji normalitas dilakukan untuk mengetahui apakah data residual dalam model regresi berdistribusi normal atau tidak. Pengujian ini menggunakan metode One-Sample Kolmogorov-Smirnov Test, dengan kriteria apabila nilai signifikansi $> 0,05$ maka

data dinyatakan berdistribusi normal. Adapun hasil uji normalitas adalah sebagai berikut:

Tabel 4. 7 Hasil Uji Normalitas (One-Sample Kolmogorov-Smirnov Test)

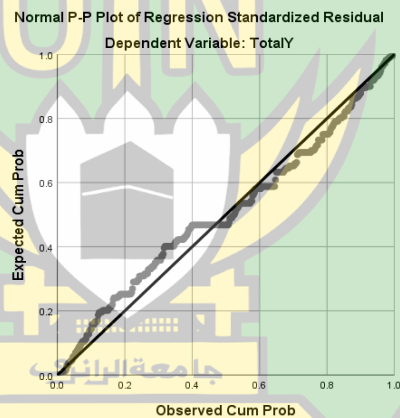
Keterangan	Unstandardized Residual
N	384
Mean	0,0000000
Std. Deviation	1,69852692
Test Statistic (Absolute)	0,083
Asymp. Sig. (2-tailed)	0,000
Monte Carlo Sig. (2-tailed)	0,008

Sumber: hasil olah data SPSS (2026)

Berdasarkan tabel 4.7, diketahui nilai Asymp. Sig. (2-tailed) sebesar 0,000 dan Monte Carlo Sig. (2-tailed) sebesar 0,008. Kedua nilai tersebut lebih kecil dari 0,05, sehingga berdasarkan kriteria pengambilan keputusan dapat disimpulkan bahwa data residual dalam model regresi penelitian ini tidak berdistribusi normal. Secara teori, apabila asumsi normalitas tidak terpenuhi, maka pengujian hipotesis seharusnya dilakukan dengan menggunakan uji statistik non-parametrik. Namun demikian, penelitian ini tetap menggunakan analisis regresi (parametrik) dengan mempertimbangkan jumlah sampel yang digunakan dalam penelitian ini, yaitu sebanyak 384 responden. Jumlah sampel yang besar tersebut ($n > 30$) memungkinkan diterapkannya konsep *Central Limit Theorem* (CLT) atau Teorema Limit Pusat, yang

menyatakan bahwa distribusi sampling dari suatu statistik, seperti nilai rata-rata atau estimator koefisien regresi, akan cenderung mendekati distribusi normal seiring bertambahnya ukuran sampel, terlepas dari bentuk distribusi populasi aslinya (Ghozali, 2021). Meskipun hasil uji Kolmogorov-Smirnov menunjukkan bahwa data residual tidak berdistribusi normal, analisis regresi dalam penelitian ini tetap dapat dikatakan *robust* (kuat) terhadap pelanggaran asumsi normalitas karena didukung oleh jumlah sampel yang besar.

Gambar 4. 7 Normal P-P Plot of Regression Standardized Residual



Hasil uji Kolmogorov-Smirnov menunjukkan nilai Asymp. Sig. sebesar 0,000, yang berarti lebih kecil dari taraf signifikansi 0,05 yang ditetapkan. Pada grafik Normal P-P Plot, terlihat bahwa sebaran titik-titik residual belum sepenuhnya merapat pada garis diagonal, dengan pola penyimpangan yang cukup terlihat pada rentang nilai tengah. Kondisi ini secara visual turut mengonfirmasi

hasil uji statistik bahwa residual belum sepenuhnya mengikuti distribusi normal. Namun demikian, penyimpangan tersebut tidak menjadi persoalan yang serius mengingat ukuran sampel penelitian yang besar ($n = 384$) memungkinkan berlakunya konsep *Central Limit Theorem*, sehingga model regresi tetap dapat digunakan secara valid.

4.5.2 Uji Multikolinearitas

Uji multikolinearitas dilakukan untuk mengetahui ada atau tidaknya korelasi antar variabel independen dalam model regresi. Multikolinearitas dapat diindikasikan apabila nilai tolerance $< 0,10$ atau nilai Variance Inflation Factor (VIF) > 10 . Adapun hasil uji multikolinearitas adalah sebagai berikut:

Tabel 4. 8 Hasil Uji Multikolinearitas

Model	Tolerance	VIF	Keterangan
Literasi Digital (X1)	0,273	3,658	Tidak terjadi multikolinearitas
Keamanan Data Pribadi (X2)	0,273	3,658	Tidak terjadi multikolinearitas

Sumber: Hasil olah data SPSS (2026)

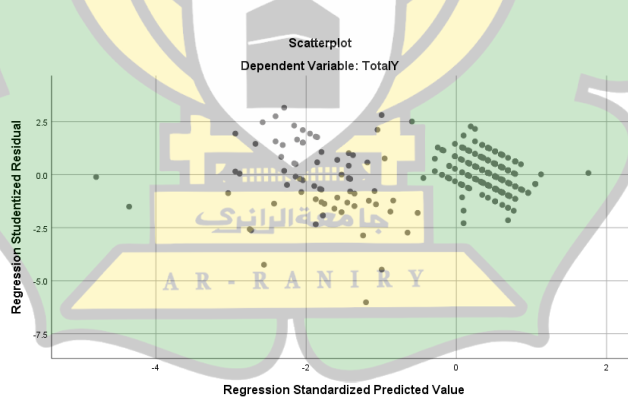
Berdasarkan tabel 4.8, diketahui bahwa nilai tolerance pada variabel Literasi Digital (X1) dan Keamanan Data Pribadi (X2) masing-masing sebesar 0,273 ($> 0,10$), sedangkan nilai VIF masing-masing sebesar 3,658 (< 10). Dengan demikian, dapat disimpulkan bahwa tidak terdapat masalah multikolinearitas antar

variabel independen dalam model regresi penelitian ini, sehingga model dinyatakan memenuhi asumsi multikolinearitas.

4.5.3 Uji Heteroskedastisitas

Uji heteroskedastisitas dilakukan untuk mengetahui apakah dalam model regresi terjadi ketidaksamaan varians residual dari satu pengamatan ke pengamatan lain. Pengujian dilakukan dengan menganalisis pola titik pada grafik scatterplot antara nilai prediksi variabel dependen dengan residualnya. Apabila titik-titik menyebar secara acak tanpa membentuk pola tertentu, baik di atas maupun di bawah angka nol pada sumbu Y, maka model dinyatakan tidak mengalami heteroskedastisitas. Adapun hasil uji heteroskedastisitas adalah sebagai berikut:

Gambar 4. 8 Hasil Uji Heteroskedastisitas (Scatterplot)



Sumber: hasil olah data SPSS (2026)

Berdasarkan Gambar 4.7, terlihat bahwa titik-titik residual menyebar di atas dan di bawah angka nol pada sumbu Y. Pada beberapa bagian terlihat adanya pengelompokan titik yang membentuk pola garis diagonal. Pola tersebut dapat muncul karena

karakteristik data penelitian yang menggunakan skala Likert dan nilai variabel yang bersifat diskrit. Meskipun demikian, secara keseluruhan scatterplot tidak menunjukkan pola sistematis berupa pola mengerucut, melebar, maupun bergelombang. Oleh karena itu, berdasarkan pemeriksaan scatterplot, belum terlihat pola yang secara jelas menunjukkan adanya heteroskedastisitas.

4.6 Hasil Uji Regresi Linear Berganda

Analisis regresi linear berganda digunakan untuk mengetahui pengaruh variabel Literasi Digital (X1) dan Keamanan Data Pribadi (X2) terhadap kewaspadaan terhadap Penipuan Digital (Y) pada nasabah Bank Aceh Syariah di Kota Banda Aceh. Adapun hasil pengujian regresi linear berganda adalah sebagai berikut:

Tabel 4. 9 Hasil Uji Regresi Linear Berganda

Model	B	Std. Error	Beta	t	Sig.
(Constant)	0,599	0,701	-	0,854	0,393
Literasi Digital (X1)	0,516	0,040	0,620	12,862	0,000
Keamanan Data Pribadi (X2)	0,287	0,050	0,279	5,787	0,000

Sumber: Hasil olah data SPSS (2026)

Berdasarkan tabel 4.9 di atas, maka dapat disusun persamaan regresi linear berganda sebagai berikut:

$$Y = \alpha + b1X1 + b2X2 + e$$

$$Y = 0,599 + 0,516X1 + 0,287X2 + e$$

Adapun interpretasi dari persamaan regresi di atas adalah sebagai berikut:

- 1) Nilai konstanta sebesar 0,599 menunjukkan bahwa apabila variabel Literasi Digital dan Keamanan Data Pribadi bernilai nol (tidak ada pengaruh), maka nilai kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh adalah sebesar 0,599.
- 2) Koefisien regresi variabel Literasi Digital (X1) bernilai positif sebesar 0,516, artinya setiap peningkatan literasi digital sebesar satu satuan akan meningkatkan nilai variabel kewaspadaan terhadap Penipuan Digital (Y) sebesar 0,516 satuan, dengan asumsi variabel lain konstan.
- 3) Koefisien regresi variabel Keamanan Data Pribadi (X2) bernilai positif sebesar 0,287, artinya setiap peningkatan keamanan data pribadi sebesar satu satuan akan meningkatkan nilai variabel kewaspadaan terhadap Penipuan Digital (Y) sebesar 0,287 satuan, dengan asumsi variabel lain konstan.

4.7 Hasil Uji Hipotesis

4.7.1 Uji Parsial (Uji t)

Uji t dilakukan untuk mengetahui pengaruh masing-masing variabel independen terhadap variabel dependen secara parsial. Pengambilan keputusan dilakukan dengan membandingkan nilai t hitung dengan t tabel pada taraf signifikansi 0,05 (5%). Nilai t tabel diperoleh melalui derajat kebebasan ($df = n - k - 1 = 384 - 2 - 1 = 381$,

yaitu sebesar 1,966. Berdasarkan tabel 4.6, hasil uji t adalah sebagai berikut:

- 1) Variabel Literasi Digital (X1) memiliki nilai t hitung sebesar 12,862 yang lebih besar dari t tabel 1,966 ($12,862 > 1,966$), dengan nilai signifikansi sebesar $0,000 < 0,05$. Dengan demikian, H1 diterima, yang berarti Literasi Digital berpengaruh signifikan terhadap kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.
- 2) Variabel Keamanan Data Pribadi (X2) memiliki nilai t hitung sebesar 5,787 yang lebih besar dari t tabel 1,966 ($5,787 > 1,966$), dengan nilai signifikansi sebesar $0,000 < 0,05$. Dengan demikian, H2 diterima, yang berarti Keamanan Data Pribadi berpengaruh signifikan terhadap kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

4.7.2 Uji Simultan (Uji F)

Uji F dilakukan untuk mengetahui apakah variabel independen secara bersama-sama (simultan) berpengaruh signifikan terhadap variabel dependen. Adapun hasil uji F adalah sebagai berikut:

Tabel 4. 10 Hasil Uji Simultan (Uji F)

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	3456,037	2	1728,018	595,840	0,000
Residual	1104,953	381	2,900	-	-
Total	4560,990	383	-	-	-

Sumber: hasil olah data SPSS (2026)

Berdasarkan tabel 4.10, diketahui nilai F hitung sebesar 595,840 dengan taraf signifikansi 0,000. Nilai F tabel pada $df_1 = 2$ dan $df_2 = 381$ dengan taraf signifikansi 5% adalah sebesar 3,019. Karena nilai F hitung lebih besar dari F tabel ($595,840 > 3,019$) dan nilai signifikansi $0,000 < 0,05$, maka H_3 diterima. Dengan demikian, dapat disimpulkan bahwa variabel Literasi Digital (X1) dan Keamanan Data Pribadi (X2) secara simultan berpengaruh signifikan terhadap kewaspadaan terhadap Penipuan Digital (Y) pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

4.7.3 Uji Determinasi (R^2)

Koefisien determinasi (R^2) digunakan untuk mengukur seberapa besar kemampuan variabel independen, yaitu Literasi Digital (X1) dan Keamanan Data Pribadi (X2), dalam menjelaskan variasi variabel dependen kewaspadaan terhadap Penipuan Digital (Y). Adapun hasil uji determinasi adalah sebagai berikut:

Tabel 4. 11 Hasil Uji Determinasi (R^2)

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0,870	0,758	0,756	1,703

Sumber: hasil olah data SPSS (2026)

Predictors: (Constant), Keamanan Data Pribadi, Literasi Digital

Berdasarkan tabel 4.8, diketahui bahwa nilai koefisien determinasi Adjusted R Square sebesar 0,756 atau 75,6%. Hal ini menunjukkan bahwa variabel Literasi Digital (X1) dan Keamanan Data Pribadi (X2) secara bersama-sama mampu menjelaskan variasi variabel kewaspadaan terhadap Penipuan Digital (Y) sebesar 75,6%, sedangkan sisanya sebesar 24,4% dijelaskan oleh variabel-variabel lain di luar model penelitian ini. Berdasarkan tinjauan pustaka, variabel yang diduga turut berpengaruh seperti perilaku pengguna, kualitas sistem keamanan platform digital, maupun faktor eksternal lain yang tidak diteliti dalam penelitian ini.

4.8 Pembahasan

Bagian ini menguraikan pembahasan atas hasil pengujian hipotesis yang telah dilakukan, dikaitkan dengan teori dan hasil penelitian terdahulu, guna menjawab rumusan masalah penelitian mengenai pengaruh Literasi Digital dan Keamanan Data Pribadi terhadap kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh.

4.8.1 Pengaruh Literasi Digital terhadap Kewaspadaan terhadap Penipuan Digital

Hasil pengujian hipotesis pertama (H1) menunjukkan bahwa Literasi Digital berpengaruh signifikan terhadap kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh, dengan nilai t hitung $12,862 > t$ tabel $1,966$ dan nilai signifikansi $0,000 < 0,05$. Koefisien regresi bernilai positif sebesar $0,516$ dengan nilai Beta sebesar $0,620$, yang menunjukkan bahwa semakin tinggi tingkat literasi digital nasabah, maka semakin tinggi pula tingkat kewaspadaan, kesadaran, dan pengetahuan nasabah terhadap berbagai bentuk rekayasa sosial dalam penipuan digital. Nilai Beta tersebut juga menunjukkan bahwa di antara kedua variabel independen, Literasi Digital memberikan kontribusi pengaruh terhadap kewaspadaan terhadap Penipuan Digital.

Berdasarkan hasil tanggapan responden pada Tabel 4.2, penguasaan Literasi Digital pada setiap indikator berbeda-beda. Nilai tertinggi terdapat pada kemampuan menggunakan kata kunci yang tepat saat mencari informasi perbankan di internet, dengan nilai rata-rata $4,31$ atau $86,20\%$. Hal ini menunjukkan bahwa sebagian besar nasabah Bank Aceh Syariah sudah mampu mencari informasi perbankan secara efektif melalui internet.

Sementara itu, nilai terendah terdapat pada kemampuan membedakan situs resmi dan situs palsu layanan perbankan digital, dengan nilai rata-rata $3,83$ atau $76,61\%$. Meskipun masih berada dalam kategori baik, hasil tersebut menunjukkan bahwa

kemampuan nasabah dalam mengenali situs palsu masih perlu ditingkatkan. Kemampuan ini penting untuk membantu nasabah menghindari tautan palsu atau phishing yang dapat digunakan oleh pelaku penipuan digital.

Jika dikaitkan dengan Protection Motivation Theory, Literasi Digital berperan dalam proses *threat appraisal*. Nasabah yang memiliki kemampuan literasi digital yang baik akan lebih mampu mengenali keberadaan, karakteristik, dan risiko dari ancaman penipuan digital. Kemampuan tersebut mendorong nasabah untuk lebih berhati-hati sebelum mempercayai informasi, mengklik tautan, atau memberikan data pribadi (Winarto & Bisma, 2021).

Dalam perspektif Islam, sebagaimana telah diuraikan pada pembahasan penipuan dalam perspektif Islam. Semakin tinggi literasi digital nasabah, semakin baik pula kemampuannya dalam mengenali berbagai bentuk *ghisy* dan *tadlīs* dalam konteks digital. *Ghisy* dapat tercermin dalam pemberian informasi palsu atau tindakan tipu daya, sedangkan *tadlīs* dapat berupa penyamaran atau manipulasi informasi, seperti penggunaan tautan *phishing*, situs palsu, maupun rekayasa sosial yang bertujuan mengelabui korban. Kemampuan untuk mengenali berbagai modus tersebut dapat membantu nasabah menghindari kerugian akibat penipuan dan melindungi hartanya dari perolehan atau penguasaan secara tidak sah. Hal ini sejalan dengan larangan memperoleh harta dengan jalan yang batil sebagaimana disebutkan dalam QS. Al-Baqarah

ayat 188. Dengan demikian, penguatan literasi digital tidak hanya bernilai strategis dalam meningkatkan kewaspadaan terhadap penipuan digital, tetapi juga sejalan dengan prinsip Islam dalam menjaga harta (*hifz al-māl*) dari berbagai bentuk penipuan dan penyalahgunaan (Eriyan et al., 2026).

Temuan ini sejalan dengan penelitian Harliani & Kurniawan (2025) yang menemukan bahwa kemampuan literasi digital memberikan pengaruh signifikan terhadap pencegahan penipuan online, dengan kontribusi sebesar 63,2% terhadap variasi pencegahan penipuan pada remaja. Hasil ini juga sejalan dengan temuan Hutagaol dkk (2024) yang menunjukkan bahwa tingkat pengetahuan keamanan siber dan perilaku pengguna berpengaruh positif dan signifikan terhadap persepsi risiko ancaman cyber crime pada pengguna mobile banking. Semakin tinggi kemampuan nasabah dalam mencari, menavigasi, mengevaluasi, dan menyusun informasi digital secara kritis, semakin besar pula kemampuan nasabah dalam mengenali dan mewaspadaai indikasi penipuan digital, seperti tautan phishing, permintaan data yang mencurigakan, maupun modus rekayasa sosial lainnya.

4.8.2 Pengaruh Keamanan Data Pribadi terhadap Kewaspadaan terhadap Penipuan Digital

Hasil pengujian hipotesis kedua (H2) menunjukkan bahwa Keamanan Data Pribadi berpengaruh signifikan terhadap kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh, dengan nilai t hitung $5,787 > t$ tabel

1,966 dan nilai signifikansi $0,000 < 0,05$. Nilai koefisien regresi sebesar 0,287 serta nilai Beta sebesar 0,279 menunjukkan bahwa variabel Keamanan Data Pribadi tetap memberikan kontribusi pengaruh yang berarti, meskipun kontribusinya lebih kecil dibandingkan variabel Literasi Digital terhadap kewaspadaan terhadap Penipuan Digital.

Berdasarkan hasil tanggapan responden pada Tabel 4.2, tingkat Literasi Digital pada setiap indikator berbeda-beda. Nilai tertinggi terdapat pada kemampuan menggunakan kata kunci yang tepat saat mencari informasi perbankan di internet, dengan nilai rata-rata 4,31 atau 86,20%. Hal ini menunjukkan bahwa sebagian besar nasabah Bank Aceh Syariah sudah mampu mencari informasi perbankan melalui internet dengan baik.

Sementara itu, nilai terendah terdapat pada kemampuan membedakan situs resmi dan situs palsu layanan perbankan digital, dengan nilai rata-rata sebesar 3,83 atau 76,61%. Meskipun masih berada dalam kategori baik, hasil ini menunjukkan bahwa kemampuan nasabah dalam mengenali situs palsu masih perlu ditingkatkan. Kemampuan tersebut penting untuk membantu nasabah mengenali indikasi phishing, termasuk tautan atau situs palsu yang dapat digunakan pelaku untuk memperoleh informasi pribadi dan melakukan penipuan digital.

Dalam Protection Motivation Theory, Keamanan Data Pribadi dapat dikaitkan dengan proses *coping appraisal*. Setelah individu menyadari adanya ancaman, individu perlu memiliki

kemampuan dan keyakinan untuk melakukan tindakan perlindungan. Perilaku menjaga PIN, kata sandi, kode OTP, dan data pribadi merupakan bentuk tindakan perlindungan yang dilakukan untuk mengurangi kemungkinan terjadinya penipuan (Winarto & Bisma, 2021).

Dalam perspektif Islam, data pribadi nasabah, seperti kata sandi, kode OTP, dan informasi identitas, merupakan amanah yang harus dijaga. Kelalaian dalam menjaga data tersebut dapat membuka peluang terjadinya *ghisy* berupa tindakan penipuan maupun *tadlīs* melalui penyamaran dan manipulasi informasi. Oleh karena itu, menjaga keamanan data pribadi tidak hanya menjadi bentuk perlindungan teknis, tetapi juga mencerminkan nilai amanah dan upaya menjaga harta (*hifz al-māl*). Dengan demikian, semakin baik penerapan keamanan data pribadi, semakin tinggi pula kewaspadaan nasabah terhadap penipuan digital (Wahyuni et al., 2025).

Temuan ini mendukung penelitian Permana dkk (2024) yang menunjukkan bahwa terdapat korelasi positif yang kuat antara persepsi keamanan data pribadi dengan kepercayaan pengguna aplikasi mobile banking, di mana sistem verifikasi berbasis teknologi seperti OTP dan biometrik memberikan dampak besar terhadap persepsi keamanan pengguna. Hal ini juga sejalan dengan penelitian Nupus dkk (2025) yang menemukan bahwa persepsi keamanan berpengaruh signifikan terhadap tingkat kepercayaan pengguna produk *e-banking* pada bank syariah. Semakin baik

pemahaman dan praktik nasabah dalam menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data pribadinya, semakin tinggi pula kesiapan dan kewaspadaan nasabah dalam menghadapi berbagai modus penipuan digital yang berupaya mengakses maupun menyalahgunakan data pribadi tersebut.

4.8.3 Pengaruh Literasi Digital dan Keamanan Data Pribadi secara Simultan terhadap Kewaspadaan terhadap Penipuan Digital

Hasil pengujian hipotesis ketiga (H3) menunjukkan bahwa Literasi Digital dan Keamanan Data Pribadi secara simultan berpengaruh signifikan terhadap kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh, dengan nilai F hitung $595,840 > F$ tabel $3,019$ dan nilai signifikansi $0,000 < 0,05$. Nilai koefisien determinasi (*Adjusted R Square*) sebesar $0,756$ menunjukkan bahwa kedua variabel independen tersebut mampu menjelaskan variasi Penipuan Digital sebesar $75,6\%$, sedangkan sisanya sebesar $24,4\%$ dipengaruhi oleh faktor lain di luar model penelitian ini.

Temuan ini sejalan dengan penelitian Yoviani dkk (2025) yang menunjukkan bahwa kemudahan, keamanan, dan literasi digital secara simultan berpengaruh positif dan signifikan terhadap perilaku nasabah dalam menggunakan layanan digital perbankan syariah. Hal ini mengindikasikan bahwa literasi digital dan keamanan data pribadi merupakan dua faktor yang saling

melengkapi dan perlu ditingkatkan secara bersamaan. Nasabah yang memiliki literasi digital yang baik namun kurang menerapkan praktik keamanan data pribadi, maupun sebaliknya, tetap berpotensi menghadapi risiko penipuan digital. Oleh karena itu, Bank Aceh Syariah perlu merancang program edukasi yang bersifat komprehensif, yang tidak hanya meningkatkan pemahaman nasabah terhadap teknologi digital, tetapi juga menanamkan kesadaran dan kebiasaan dalam menjaga keamanan data pribadi, sehingga dapat menekan tingkat kerentanan nasabah terhadap kewaspadaan terhadap penipuan digital secara berkelanjutan.

Hasil penelitian ini sesuai dengan Protection Motivation Theory, yang menjelaskan bahwa perilaku perlindungan terbentuk melalui dua proses, yaitu *threat appraisal* dan *coping appraisal*. Dalam penelitian ini, Literasi Digital membantu nasabah mengenali dan menilai ancaman penipuan digital, sedangkan Keamanan Data Pribadi mencerminkan tindakan perlindungan yang dilakukan nasabah untuk mengurangi risiko tersebut. Kedua proses tersebut secara bersama-sama membentuk kewaspadaan terhadap penipuan digital (Winarto & Bisma, 2021).

Hasil pengujian pengaruh Literasi Digital dan Keamanan Data Pribadi secara terhadap Kewaspadaan terhadap Penipuan Digital dapat dikaitkan dengan perspektif Islam. Literasi digital membantu nasabah mengenali berbagai bentuk *ghisy* berupa tipu daya dan *tadlīs* melalui penyamaran atau manipulasi informasi, sedangkan keamanan data pribadi menjadi bentuk ikhtiar dalam

menjaga informasi dan mencegah penyalahgunaannya. Kedua hal tersebut tidak hanya meningkatkan kewaspadaan nasabah terhadap penipuan digital, tetapi juga sejalan dengan nilai kehati-hatian, amanah, dan upaya menjaga harta (*hifz al-māl*) dalam Islam. Dengan demikian, semakin baik literasi digital dan penerapan keamanan data pribadi secara bersama-sama, semakin tinggi pula kewaspadaan nasabah dalam menghadapi berbagai modus penipuan digital.

Hasil penelitian ini menunjukkan bahwa kewaspadaan terhadap penipuan digital tidak hanya dipengaruhi oleh satu faktor saja, melainkan dari penggabungan kemampuan literasi digital dan praktik keamanan data pribadi yang dijalankan oleh nasabah. Kedua variabel tersebut saling melengkapi, dimana literasi digital berkaitan dengan kemampuan nasabah dalam mengenali dan menilai ancaman, sedangkan keamanan data pribadi berkaitan dengan tindakan nyata yang dilakukan untuk melindungi diri dari ancaman tersebut. Nasabah yang memiliki literasi digital yang baik namun kurang menerapkan praktik keamanan data pribadi, maupun sebaliknya, tetap berpotensi menghadapi risiko penipuan digital.

Sejalan dengan itu, pada variabel kewaspadaan terhadap Penipuan Digital (Tabel 4.4) terlihat bahwa item yang memperoleh nilai tertinggi terdapat pada kehati-hatian nasabah terhadap pesan atau telepon yang mengatasnamakan pihak bank, dengan nilai rata-rata 4,21 atau 84,27%. Hal ini menunjukkan bahwa nasabah secara umum sudah cukup waspada terhadap modus komunikasi yang

paling umum digunakan pelaku penipuan. Di sisi lain, nilai terendah terdapat pada kesadaran bahwa pelaku penipuan dapat mengatasnamakan pihak bank untuk memperoleh data pribadi nasabah, dengan nilai rata-rata 3,90 atau 77,92%. Hal ini mengindikasikan bahwa meskipun nasabah cukup berhati-hati secara umum, pemahaman terhadap taktik spesifik pelaku penipuan digital masih perlu diperkuat melalui edukasi yang lebih menasar pada pengenalan modus operandi.

Hasil penelitian ini sesuai dengan *Protection Motivation Theory*, yang menjelaskan bahwa perilaku perlindungan terbentuk melalui dua proses, yaitu *threat appraisal* dan *coping appraisal*. Dalam penelitian ini, Literasi Digital membantu nasabah mengenali dan menilai ancaman penipuan digital, sedangkan Keamanan Data Pribadi mencerminkan tindakan perlindungan yang dilakukan nasabah untuk mengurangi risiko tersebut. Kedua proses tersebut secara bersama-sama membentuk kewaspadaan terhadap penipuan digital (Winarto & Bisma, 2021).

Apabila dikaitkan dengan perspektif Islam, literasi digital membantu nasabah mengenali berbagai bentuk *ghisy* berupa tipu daya dan *tadlis* melalui penyamaran atau manipulasi informasi, sedangkan keamanan data pribadi menjadi bentuk ikhtiar dalam menjaga informasi dan mencegah penyalahgunaannya. Kedua hal tersebut tidak hanya meningkatkan kewaspadaan nasabah terhadap penipuan digital, tetapi juga sejalan dengan nilai kehati-hatian, amanah, dan upaya menjaga harta (*hifz al-māl*) dalam Islam.

Temuan ini sejalan dengan penelitian Yoviani dkk (2025) yang menunjukkan bahwa kemudahan, keamanan, dan literasi digital secara simultan berpengaruh positif dan signifikan terhadap perilaku nasabah dalam menggunakan layanan digital perbankan syariah, di mana perilaku tersebut tidak terlepas dari tingkat kewaspadaan nasabah terhadap risiko penipuan digital yang mungkin timbul dalam penggunaan layanan tersebut. Hal ini mengindikasikan bahwa literasi digital dan keamanan data pribadi merupakan dua faktor yang saling melengkapi dan perlu ditingkatkan secara bersamaan. Oleh karena itu, Bank Aceh Syariah perlu merancang program edukasi yang bersifat komprehensif, yang tidak hanya meningkatkan pemahaman nasabah terhadap teknologi digital, tetapi juga menanamkan kesadaran dan kebiasaan dalam menjaga keamanan data pribadi, sehingga dapat menekan tingkat kerentanan nasabah terhadap penipuan digital secara berkelanjutan.

Berdasarkan keseluruhan pembahasan di atas, dapat dipahami bahwa Literasi Digital dan Keamanan Data Pribadi secara simultan berpengaruh positif dan signifikan terhadap kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh. Selain dari hasil uji statistik, pengaruh tersebut juga terlihat dari kecenderungan jawaban responden yang menekankan pada kemampuan mencari informasi secara efektif dan kesadaran menjaga kerahasiaan kredensial akun. Dengan demikian, semakin tinggi literasi digital yang dimiliki serta

semakin baik praktik keamanan data pribadi yang diterapkan nasabah, maka semakin tinggi pula kewaspadaan nasabah dalam menghadapi berbagai modus penipuan digital.



BAB V

PENUTUP

5.1 Kesimpulan

Penelitian ini bertujuan untuk menganalisis pengaruh Literasi Digital dan Keamanan Data Pribadi terhadap kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh, baik secara parsial maupun simultan. Berdasarkan hasil pengolahan dan analisis data yang telah diuraikan pada bab sebelumnya, dapat ditarik kesimpulan sebagai berikut:

- 1) Literasi Digital terbukti berpengaruh positif dan signifikan terhadap Kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh, sehingga hipotesis pertama (H1) diterima ($t_{hitung} 12,862 > t_{tabel} 1,966$; sig. 0,000). Pengaruh Literasi Digital juga tercatat paling dominan di antara kedua variabel bebas (Beta 0,620). Artinya, semakin tinggi kemampuan nasabah dalam mencari, menyaring, dan mengevaluasi informasi digital, semakin tinggi pula kewaspadaan dan kemampuannya mengenali indikasi penipuan digital, seperti tautan phishing maupun rekayasa sosial, sehingga literasi digital menjadi faktor kunci dalam melindungi nasabah dari ancaman penipuan digital.
- 2) Keamanan Data Pribadi terbukti berpengaruh positif dan signifikan terhadap Kewaspadaan Terhadap Penipuan

Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh, sehingga hipotesis kedua (H2) diterima (t hitung $5,787 > t$ tabel $1,966$; sig. $0,000$). Nilai Beta sebesar $0,279$ menunjukkan bahwa kontribusi pengaruh Keamanan Data Pribadi lebih rendah dibandingkan Literasi Digital. Artinya, semakin baik penerapan keamanan data pribadi oleh nasabah, seperti menjaga kerahasiaan kata sandi, kode OTP, dan data pribadi lainnya, semakin tinggi pula kewaspadaan nasabah terhadap potensi penipuan digital, sehingga keamanan data pribadi turut berperan penting dalam melindungi nasabah dari ancaman penipuan digital.

- 3) Literasi Digital dan Keamanan Data Pribadi juga terbukti berpengaruh signifikan secara simultan terhadap Kewaspadaan terhadap Penipuan Digital pada nasabah Bank Aceh Syariah di Kota Banda Aceh, sehingga hipotesis ketiga (H3) diterima (F hitung $595,840 > F$ tabel $3,019$; sig. $0,000$). Kedua variabel ini secara bersama-sama mampu menjelaskan sebagian besar variasi Penipuan Digital (Adjusted R Square $75,6\%$), sedangkan sisanya dijelaskan oleh faktor lain di luar model, seperti perilaku pengguna, kualitas sistem keamanan platform digital, maupun faktor eksternal lainnya. Artinya, Literasi Digital dan Keamanan Data Pribadi merupakan dua faktor yang saling melengkapi dan perlu ditingkatkan secara bersamaan agar upaya

pencegahan penipuan digital pada nasabah dapat berjalan lebih efektif.

5.2 Saran

Berdasarkan kesimpulan di atas, maka peneliti mengajukan beberapa saran sebagai berikut:

1. Bagi Bank Aceh Syariah

Bank Aceh Syariah disarankan untuk rutin memberikan edukasi dan sosialisasi literasi digital kepada nasabah melalui media sosial, aplikasi mobile banking, maupun kegiatan tatap muka. Edukasi perlu difokuskan pada pengenalan modus penipuan digital, seperti phishing dan rekayasa sosial. Mengingat kemampuan nasabah dalam membedakan situs resmi dan situs palsu masih relatif rendah, bank perlu memberikan panduan praktis mengenai ciri-ciri tautan, aplikasi, dan situs resmi perbankan. Sosialisasi mengenai penipuan yang mengatasnamakan pihak bank juga perlu ditingkatkan agar nasabah tidak mudah percaya kepada pihak yang mengaku sebagai bank. Mengingat mayoritas responden berusia 17–25 tahun dan berstatus mahasiswa serta pegawai swasta, edukasi sebaiknya disampaikan melalui kanal yang sering digunakan kelompok tersebut, khususnya media sosial dan aplikasi mobile banking, sehingga informasi lebih mudah diterima dan tepat sasaran.

2. Bagi Nasabah Bank Aceh Syariah

Nasabah disarankan untuk terus meningkatkan literasi digital secara mandiri, seperti mengikuti perkembangan informasi mengenai keamanan siber dan modus penipuan digital terbaru, serta lebih berhati-hati dan selektif dalam menerima tautan, pesan, atau permintaan data pribadi yang mencurigakan. Nasabah juga disarankan untuk senantiasa menjaga kerahasiaan data pribadi dan kredensial akun perbankan digitalnya guna meminimalkan risiko menjadi korban penipuan digital.

3. Bagi Regulator/Otoritas Jasa Keuangan (OJK)

Otoritas Jasa Keuangan (OJK) dan regulator terkait disarankan untuk terus memperkuat regulasi perlindungan data pribadi nasabah di sektor perbankan syariah, serta mendorong bank untuk menerapkan standar keamanan sistem digital yang lebih ketat, misalnya melalui verifikasi berlapis dan pemantauan transaksi mencurigakan. Selain itu, regulator disarankan untuk menggalakkan kampanye literasi digital dan keamanan siber secara berkelanjutan, baik di tingkat nasional maupun daerah, guna menekan angka penipuan digital yang menyasar nasabah perbankan syariah.

4. Bagi Peneliti Selanjutnya

Mengingat nilai Adjusted R Square sebesar 75,6%, masih terdapat 24,4% variasi Penipuan Digital yang dipengaruhi

faktor lain di luar model. Oleh karena itu, peneliti selanjutnya disarankan menambahkan variabel lain, seperti kepercayaan, perilaku pengguna, kualitas sistem keamanan platform digital, dan religiusitas. Penelitian juga dapat diperluas dengan melibatkan bank syariah lain, wilayah yang lebih luas, dan jumlah sampel yang lebih besar agar hasilnya lebih representatif. Selain itu, penelitian selanjutnya dapat mengkaji lebih lanjut aspek yang memperoleh skor relatif rendah, yaitu kemampuan membedakan situs resmi dan palsu (76,61%), tanggung jawab menjaga kerahasiaan data pribadi (77,76%), serta kesadaran terhadap penipuan yang mengatasnamakan pihak bank (77,92%). Pengkajian dapat dilakukan melalui pendekatan kualitatif atau wawancara mendalam untuk mengetahui penyebab rendahnya aspek tersebut dan merumuskan strategi edukasi serta mitigasi penipuan digital yang lebih tepat sasaran bagi nasabah perbankan syariah.

DAFTAR PUSTAKA

- Amri, N. F., Anwar, C. R., & Monoarfa, M. (2024). *Analisis Literasi Digital Dalam Pembelajaran Mahasiswa Angkatan 2021 Prodi Teknologi Pendidikan Fakultas Ilmu Pendidikan Universitas Negeri Makassar*. 4(2).
- Amzah, R. A., Fitri, L. E., & Lubis, P. (2024). Analisis Pengaruh Kualitas Layanan Dan Presepsi Cybercrime Terhadap Loyalitas Nasabah Pengguna E-Banking Pada Bank Syariah Indonesia Kota Jambi. *Bertuah Jurnal Syariah Dan Ekonomi Islam*, 5(2), 229–238.
- Analisaaceh.Com. (2025). *Penipuan Catut Nama Ketua Pwi Aceh, Korban Transfer Rp35 Juta*. Analisaaceh.Com.
- Anindya, T. D., Sasmita, G. M. A., & Pratama, I. P. A. E. (2023). *Edukasi Bahaya Social Engineering Menggunakan Media Belajar Quizizz Untuk Meningkatkan Kesadaran Keamanan Informasi Nasabah Perbankan*. 4(3).
- Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2025). *Penyalahgunaan Data Pribadi Dalam Teknologi Transaksi Digital Di Industri Perbankan Digital (Studi Kasus Pt . Bank Syariah Indonesia)*. 2(1), 316–327.
- Ari, M., Nurkhozin, & Setiawati, P. C. (2024). *Persepsi Nasabah Terhadap Kualitas Pelayanan Di Bank Syariah Indonesia*. 2, 34–47.
- Ariani, R., Kusumarani, R., & Parlina, A. (2023). *Pengukuran*

- Indeks Literasi Digital Di Perpustakaan Khusus Indonesia Berdasarkan Peraturan Perpustakaan Nasional Republik Indonesia Nomor 7 Tahun 2022 , Penelitiannya Menempatkan Peran Perpustakaan Sebagai Media Literasi Digital Masyarakat . Masyarakat Pad. 30(1), 56–67. <https://doi.org/10.37014/medpus.V30i1.3472>*
- Azzahra, E. A., & Nurkhaerani, E. (2024). *Analisis Yuridis Kebocoran Data LinkedIn 2021 Dalam Kerangka UU Perlindungan Data Pribadi Indonesia*. 4.
- Bodhi, S., & Tan, D. (2022). *Keamanan Data Pribadi Dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan Dan Pengelabuan*. 4(3), 297–308.
- Bua, I. T., & Idris, N. I. (2025). *Analisis Kebijakan Keamanan Siber Di Indonesia : Studi Kasus Kebocoran Data Nasional Pada Tahun 2024*. 2.
- Cosgrove, J., & Cachia, R. (2025). *European Digital Competence Framework*. <https://doi.org/10.2760/7379058>
- Efendi, N. A., Harahap, M. I., & Syahbundi, M. (2025). *Pengaruh Social Engineering Dan Cyber Crime Terhadap Persepsi Keamanan Pada Aplikasi Bsi Mobile*. 14(03), 1237–1250.
- Erfiana, R. N. (2023). *Pengaruh Cyber Crime Dan Ebanking Terhadap Kepuasan Nasabah Bsi (Studi Kasus Mahasiswa Solo Raya)*.
- Eriyan, M., Kholid, M., & Sumardi, D. (2026). *Penegakan Hukum Tindak Pidana Penipuan Online Melalui Media Sosial Di*

- Polda Jabar Perspektif Hukum Pidana Islam Law*. 7(1), 21–37. <https://doi.org/10.36701/Bustanul.V7i1.2959>
- Fadillah, M. A. Al, Ramadhan, M. G., & Erza, M. (2024). *Analisis Ancaman Phishing Terhadap Penggunaan E-Commerce Di Indonesia*. 5(2), 85–96.
- Ferdiansyah, Zainuddin, & Risma, A. (2025). *Perlindungan Hukum Kerahasiaan Data Pribadi Nasabah Pada Perbankan Di Indonesia*. 6, 84–94.
- Fikri, M., & Rusdiana, S. (2023). *Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia*. 5(1), 39–57.
- Gasa. (2025). *State Of Scams In Indonesia 2025 Report*. Global Anti-Scam Alliance. <https://www.gasa.org/research>
- Ghozali, I. (2021). *Aplikasi Analisis Multivariate Dengan Program Ibm Spss 26* (10th Ed.). Badan Penerbit Universitas Diponegoro.
- Gisatriadi, N. (2024). *Perkembangan Perbankan Syariah Di Era Digital*. 3(2), 216–231.
- Gunawan, D., Wibawa, M. B., Payana, M. D., & Helinda, A. (2024). *Pelatihan Literasi Digital Dan Keamanan Data Bagi Umkm*. 1–7.
- Hapsari, R. D., & Pambayun, K. G. (2023). *Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis*. *Jurnal Konstituen*, 5(1), 1–17.
- Harahap, A. H., Andani, C. D., Christie, A., & Fauzi, A. (2023).

- Pentingnya Peranan Cia Triad Dalam Keamanan Informasi Dan Data Untuk Pemangku Kepentingan Atau Stakholder. 1(2), 73–83.*
- Harliani, S., & Kurniawan, F. (2025). *Pengaruh Kemampuan Literasi Digital Terhadap Pencegahan Penipuan Online Pada Remaja Desa Saentis. 4(4), 2234–2248.*
- Hartono, C., & Keni, K. (2025). *Kesetiaan Nasabah Terhadap Bank Umum Swasta Pada Era Perkembangan Pesat Bank Digital Dan Finance Technology. 9(1), 245–260.*
- Hobbs, R. (2017). *Create To Learn: Introduction To Digital Literacy.* John Wiley & Sons.
- Hutagaol, B. J., Sitorus, R. S., & Hutagaol, N. (2024). Identifikasi Tingkat Kesadaran Pengguna Mobile Banking Terhadap Ancaman Cybercrime. *Jurnal Teknologi Sistem Informasi Dan Aplikasi, 7(3), 1043–1054.*
- Ibrahim, A. (2023). *Metodologi Penelitian Ekonomi Dan Bisnis Islam.* Bumi Aksara.
<https://books.google.co.id/books?id=T33meaaqbaj>
- Jannah, S., Maulana, M. A. R., & Khairunnisa, D. (2024). *Peran Penting Literasi Digital Dalam Pendidikan. 2(4), 16–23.*
- Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., & Afni, N. (2023). *Analisis Keamanan Data Pribadi Pada Pengguna E-Commerce : Ancaman , Risiko , Strategi Kemanan (Literature Review). August.*
<https://doi.org/10.31933/jimt.v4i5>

- Kurnia, N., Rahayu, Wendratama, E., Monggilo, Z. M. Z., Damayanti, A., Angendari, D. A. D., & Abisono, F. Q. (2022). *Penipuan Digital Di Indonesia*. Program Studi Magister Ilmu Komunikasi Fakultas Ilmu Sosial Dan Ilmu Politik Universitas Gadjah Mada.
- Maharan, A. P., Rivai, M., Sugianti, S., Fauzi, R. A. F. A., Azzahra, S., Ningsih, S., Lailiya, U., Adawiyah, R., Amalia, N. D. D., & Sudirman, S. (2021). Literasi Digital: Efektifitas Aplikasi Pedulilindungi Dalam Memberikan Informasi Pada Mahasiswa Fip Upi. *Indonesian Journal Of Adult And Community Education*, 3(2), 1–6.
- Maharani, A. C., & Purwanto, I. W. N. (2025). *Analisis Tanggung Jawab Bank Dalam Perlindungan Data Nasabah: Studi Kasus Perbankan Konvensional Dan Perbankan Digital*.
- Maulidiyah, M., Khoiriyah, E. Z., Putri, D. C., & Nurafini, F. (2024). *Analisis Faktor Yang Mempengaruhi Minat Masyarakat Lamongan Menjadi Nasabah Bank Syariah*. 7, 205–213.
- Megawati, I. A. P., & Kertiriasih, N. N. R. (2024). *Dampak Layanan Perbankan Digital Terhadap Kinerja Perbankan Di Indonesia*. 13(September), 1578–1591. <https://doi.org/10.34127/Jrlab.V13i3.1205>
- Modusaceh.Co. (2025). *Maraknya Penipuan Mengatasnamakan Bank Aceh, Nasabah Diminta Waspada*. Modusaceh.Co. <https://modusaceh.co/news/maraknya-penipuan->

Mengatasnamakan-Bank-Aceh-Nasabah-Diminta-
Waspada/Index.Html#Google_Vignette

- Mulyadi, D., Mulyana, A., Carmenita, A., Utami, H. L., Aulia, K. A., Putri, M., & Alia, N. R. (2026). *Implementasi Kebijakan Pemerintah Terhadap Pencegahan Kebocoran Data Pribadi Dalam Pelayanan Publik Berbasis Digital*. 1, 1–15.
- Napitupulu, D. A. A., & Susanti, S. (2025). Pengaruh Pelatihan Peningkatan Kemampuan Literasi Digital Ibu Rumah Tangga Terhadap Pencegahan Penipuan Online Di Kelurahan Bunga Tanjung Kota Tanjung Balai. *Pendas: Jurnal Ilmiah Pendidikan Dasar*, 10(04), 250–261.
- Naufal, H. A. (2021). *Literasi Digital. Perspektif*, 1 (2), 195–202.
- Nisa, K., Purwono, Handayani, O. P., & Setiawan. (2025). *Peningkatan Literasi Digital: Edukasi Kejahatan Siber Dan Pinjaman Online Illegal Man 2 Cilacap*. 0(0). <https://doi.org/10.35960/Pimas.V4i2.1831>
- Nupus, H., Kartini, A., & Desiana, L. (2025). Pengaruh Cyber Crime Dan Persepsi Keamanan Terhadap Tingkat Kepercayaan Pengguna Produk E-Banking (Survei Pada Pengguna E-Banking Bank Syariah Di Indonesia). *Jurnal Semesta Ilmu Manajemen Dan Ekonomi*, 1(3), 102–116.
- Nur'aini, R. J., & Simanjuntak, M. (2025). *Phishing Awareness And Security Concerns: Analyzing The Role Of Anti-Phishing Knowledge And Internet Experience In Online Banking Users*. 18(2), 121–133.

- Nur, F. (2025). *Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Penipuan Online Dengan Modus Social Engineering*. 5.
- Ojk. (2025). *Satgas Pasti Imbau Masyarakat Waspada Penipuan Menggunakan Artificial Intelligence*. Ojk. <https://www.ojk.go.id/Id/Berita-Dan-Kegiatan/Info-Terkini/Pages/Satgas-Pasti-Imbau-Masyarakat-Waspada-Penipuan-Menggunakan-Ai.aspx>
- Permana, K. K., Eprianto, I., Fauzi, A., Minarny, T., & Fajriansyah, D. N. (2024). *Pengaruh Keamanan Data Pribadi Terhadap Kepercayaan Pengguna Di Era Transformasi Digital : Studi Kasus Pada Aplikasi Mobile Banking*. 1(1), 37–46.
- Pradana, M. A. E., & Saragih, H. (2024). *Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap Gdpr Dan Akibat Hukumnya*. 4, 3412–3425.
- Prasetya, I. A., Hermanto, Sujatmiko, W., Wulandari, M., & Dzulqarnain, M. F. (2025). *Mewujudkan Kesadaran Keamanan Data Pribadi Pada Masyarakat Di Era Teknologi Informasi*. 6(September).
- Prasetyo, W. (2024). *Perlindungan Hukum Atas Data Pribadi Nasabah Dalam Penyelenggaraan Layanan Internet Banking Dihubungkan Dengan Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan*. 8(10), 34819–34825.

- Putra, F. A. N., Avanza, D. T., Asyifa, S. T., & Wahyuni, D. A. (2025). *Literasi Keamanan Data Pribadi Dan Privasi Digital*. 02(03), 2534–2536.
- Rahmah, A. T., & Fasa, M. I. (2024). *Pengaruh Transformasi Digital Dan Pengembangan Financial Technology (Fintech) Terhadap Inovasi Layanan Perbankan Syariah*. 2(3).
- Rahman, F. (2021). *Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia*.
- Reihandho, M. I., & Fajarwati, D. (2020). *Faktor-Faktor Yang Mempengaruhi Niat Penggunaan Perbankan Digital Di Indonesia Faktor-Faktor Yang Mempengaruhi Niat Penggunaan Perbankan Digital Di Indonesia*.
- Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). *Computers & Security Which Factors Predict Susceptibility To Phishing ? An Empirical Study*. 136(September 2023). <https://doi.org/10.1016/j.cose.2023.103558>
- Rizal, C., Rosyidah, U. A., Yusnanto, T., Akbar, M. R., Hidayat, L., Setiawan, J., Ilham, A., Yunus, R., Wardhani, A. K., Rahajeng, E., Nay, F. A., Irawan, J. D., Muflihah, Y., & Asari, A. (2022). *Literasi Digital*.
- Rozi, F., & Samingan, A. (2024). *Syariah Kc Solo Dengan Kepuasan Sebagai Variabel*. 4(1), 95–104.
- Sahfitri, A., & Rosmalinda, R. (2024). *Penipuan Digital Melalui*

- Tautan Phishing. *Jurnal Dialektika Hukum*, 6(2), 92–107.
- Sembiring, E. R. 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 Sosial*, 5(4), 880–887.
- Serambinews.Com. (2025). *Marak Kasus Penipuan Online Di Banda Aceh Polresta Beri Warning Warga Untuk Tidak Terjebak*. Serambinews.Com.
<https://aceh.tribunnews.com/2025/06/17/Marak-Kasus-Penipuan-Online-Di-Banda-Aceh-Polresta-Beri-Warning-Warga-Untuk-Tidak-Terjebak>
- Siagian, Y., Syah, A. Z., & Irawati, N. (2024). Peningkatan Kesadaran Dan Kewaspadaan Terhadap Ancaman Cybercrime Bagi Masyarakat Di Era Digital. *Jurnal Pengabdian Masyarakat Mitra Kreasi Cendekia (Mkc)*, 2(2), 164–169.
- Siahaan, P. G., Purba, N. R., Ritonga, N., & Silalahi, E. (2024). *Perlindungan Data Pribadi Terhadap Penanggulangan Tindakan Penipuan Online*. 9(1), 47–58.
- Sianturi, B. F. C. L., Alfian, R., Anendri, N. T., Fiyona, P., & Hidayat, M. F. (2024). *Perlindungan Hukum Terhadap Nasabah Bank Terkait Transaksi Digital Di Indonesia*. 1(4), 267–271.
- Sitompul, K. L. (2024). *Review: Analisis Faktor Yang*

Mempengaruhi Kemampuan Literasi Digital.

- Suari, K. R. A., & Sarjana, I. M. (2023). *Menjaga Privasi Di Era Digital : Perlindungan Data Pribadi Di Indonesia*. 1, 132–146. <https://doi.org/10.38043/Jah.V6i1.4484>
- Sugiyono. (2023). *Metode Penelitian Kuantitatif, Kualitatif Dan R&D*. Alfabeta.
- Suvil, A. A., Firdaus, Ramadhan, M. A., Putra, W. D., & Lestari, D. P. (2024). *Implementasi Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 11 Tahun 2020*. 3(4).
- Syafitri, N., & Agustin, G. (2023). *Social Engineering Swot Analysis In Government-Owned Commercial Banks And National Private Commercial Banks Department Of Development Economics , Faculty Of Economics And Business , Universitas Negeri Malang*. 265–281.
- Syahrin, A., Mahlizar, & Sulfitra. (2025). Pengaruh Literasi Keuangan, Kemudahan, Dan Keamanan Terhadap Keputusan Bertransaksi Menggunakan Qris Pada Umkm Di Bsi Umkm Center Aceh: Pengaruh Literasi Keuangan, Kemudahan, Dan Keamanan Terhadap Keputusan Bertransaksi Menggunakan Qris Pada Umkm Di Bsi U. *Journal Islamic Economics Ad Diwan*, 4(2), 140–146.
- Tiffani, I. (2023). *Pengaruh Literasi Keuangan Dan Literasi Digital Terhadap Preferensi Bank Digital*. 22(1), 152–167.
- Wahib, P., Narotama, A. T., Rijki, N. M., Permana, F., Sagara, D., Azkhal, D. I., Anwar, M., & Juniawan, M. R. (2022).

- Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital. *Abdi Jurnal Publikasi*, 1(2), 64–68.
- Wahyuni, Y., Sartika, S. A., Marlina, L., & Siliwangi, U. (2025). *Analisis Maraknya Penipuan Bisnis Scam Di Aplikasi Telegram Pada Perspektif Islam*. 02(02).
- Wiguna, K. A., Gadjah, U., & Yogyakarta, M. (2023). *Analisis Kompetensi Literasi Digital Pada Guru Sekolah Menengah Atas*. 21–32.
- Winarto, S. R., & Bisma, R. (2021). *Studi Literatur : Analisis Persepsi Umkm Di Indonesia Terhadap Cyber Security Menggunakan Model Protection Motivation Theory (Pmt)*. 03, 20–28.
- Yoviani, T., Dewi, A., & Ibnu, A. R. (2025). *Pengaruh Kemudahan, Keamanan Dan Literasi Digital Terhadap Minat Nasabah Menggunakan Aplikasi Muamalat Din*. 3(4), 324–336.
- Amri, N. F., Anwar, C. R., & Monoarfa, M. (2024). *Analisis Literasi Digital Dalam Pembelajaran Mahasiswa Angkatan 2021 Prodi Teknologi Pendidikan Fakultas Ilmu Pendidikan Universitas Negeri Makassar*. 4(2).
- Amzah, R. A., Fitri, L. E., & Lubis, P. (2024). *Analisis Pengaruh Kualitas Layanan Dan Presepsi Cybercrime Terhadap Loyalitas Nasabah Pengguna E-Banking Pada Bank Syariah Indonesia Kota Jambi*. *Bertuah Jurnal Syariah Dan Ekonomi Islam*, 5(2), 229–238.

- Analisaaceh.Com. (2025). *Penipuan Catut Nama Ketua Pwi Aceh, Korban Transfer Rp35 Juta*. Analisaaceh.Com.
- Anindya, T. D., Sasmita, G. M. A., & Pratama, I. P. A. E. (2023). *Edukasi Bahaya Social Engineering Menggunakan Media Belajar Quizizz Untuk Meningkatkan Kesadaran Keamanan Informasi Nasabah Perbankan*. 4(3).
- Antoine, R. A., Farizqa, N. S., Hasna, A. H., & Pasaribu, M. (2025). *Penyalahgunaan Data Pribadi Dalam Teknologi Transaksi Digital Di Industri Perbankan Digital (Studi Kasus Pt . Bank Syariah Indonesia)*. 2(1), 316–327.
- Ari, M., Nurkhozin, & Setiawati, P. C. (2024). *Persepsi Nasabah Terhadap Kualitas Pelayanan Di Bank Syariah Indonesia*. 2, 34–47.
- Ariani, R., Kusumarani, R., & Parlina, A. (2023). *Pengukuran Indeks Literasi Digital Di Perpustakaan Khusus Indonesia Berdasarkan Peraturan Perpustakaan Nasional Republik Indonesia Nomor 7 Tahun 2022 , Penelitiannya Menempatkan Peran Perpustakaan Sebagai Media Literasi Digital Masyarakat . Masyarakat Pad*. 30(1), 56–67.
<https://doi.org/10.37014/Medpus.V30i1.3472>
- Azzahra, E. A., & Nurkhaerani, E. (2024). *Analisis Yuridis Kebocoran Data LinkedIn 2021 Dalam Kerangka Uu Perlindungan Data Pribadi Indonesia*. 4.
- Bodhi, S., & Tan, D. (2022). *Keamanan Data Pribadi Dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan*

Dan Pengelabuan. 4(3), 297–308.

- Bua, I. T., & Idris, N. I. (2025). *Analisis Kebijakan Keamanan Siber Di Indonesia : Studi Kasus Kebocoran Data Nasional Pada Tahun 2024. 2.*
- Cosgrove, J., & Cachia, R. (2025). *European Digital Competence Framework. <https://doi.org/10.2760/7379058>*
- Efendi, N. A., Harahap, M. I., & Syahbundi, M. (2025). *Pengaruh Social Engineering Dan Cyber Crime Terhadap Persepsi Keamanan Pada Aplikasi Bsi Mobile. 14(03), 1237–1250.*
- Erfiana, R. N. (2023). *Pengaruh Cyber Crime Dan Ebanking Terhadap Kepuasan Nasabah Bsi (Studi Kasus Mahasiswa Solo Raya).*
- Eriyan, M., Kholid, M., & Sumardi, D. (2026). *Penegakan Hukum Tindak Pidana Penipuan Online Melalui Media Sosial Di Polda Jabar Perspektif Hukum Pidana Islam Law. 7(1), 21–37. <https://doi.org/10.36701/Bustanul.V7i1.2959>*
- Fadillah, M. A. Al, Ramadhan, M. G., & Erza, M. (2024). *Analisis Ancaman Phishing Terhadap Penggunaan E-Commerce Di Indonesia. 5(2), 85–96.*
- Ferdiansyah, Zainuddin, & Risma, A. (2025). *Perlindungan Hukum Kerahasiaan Data Pribadi Nasabah Pada Perbankan Di Indonesia. 6, 84–94.*
- Fikri, M., & Rusdiana, S. (2023). *Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. 5(1), 39–57.*

- Gasa. (2025). *State Of Scams In Indonesia 2025 Report*. Global Anti-Scam Alliance. <https://www.gasa.org/research>
- Ghozali, I. (2021). *Aplikasi Analisis Multivariate Dengan Program Ibm Spss 26* (10th Ed.). Badan Penerbit Universitas Diponegoro.
- Gisatriadi, N. (2024). *Perkembangan Perbankan Syariah Di Era Digital*. 3(2), 216–231.
- Gunawan, D., Wibawa, M. B., Payana, M. D., & Helinda, A. (2024). *Pelatihan Literasi Digital Dan Keamanan Data Bagi Umkm*. 1–7.
- Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, 5(1), 1–17.
- Harahap, A. H., Andani, C. D., Christie, A., & Fauzi, A. (2023). *Pentingnya Peranan Cia Triad Dalam Keamanan Informasi Dan Data Untuk Pemangku Kepentingan Atau Stakholder*. 1(2), 73–83.
- Harliani, S., & Kurniawan, F. (2025). *Pengaruh Kemampuan Literasi Digital Terhadap Pencegahan Penipuan Online Pada Remaja Desa Saentis*. 4(4), 2234–2248.
- Hartono, C., & Keni, K. (2025). *Kesetiaan Nasabah Terhadap Bank Umum Swasta Pada Era Perkembangan Pesat Bank Digital Dan Finance Technology*. 9(1), 245–260.
- Hobbs, R. (2017). *Create To Learn: Introduction To Digital Literacy*. John Wiley & Sons.

- Hutagaol, B. J., Sitorus, R. S., & Hutagaol, N. (2024). Identifikasi Tingkat Kesadaran Pengguna Mobile Banking Terhadap Ancaman Cybercrime. *Jurnal Teknologi Sistem Informasi Dan Aplikasi*, 7(3), 1043–1054.
- Ibrahim, A. (2023). *Metodologi Penelitian Ekonomi Dan Bisnis Islam*. Bumi Aksara.
<https://books.google.co.id/books?id=T33meaaqbaj>
- Jannah, S., Maulana, M. A. R., & Khairunnisa, D. (2024). *Peran Penting Literasi Digital Dalam Pendidikan*. 2(4), 16–23.
- Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., & Afni, N. (2023). *Analisis Keamanan Data Pribadi Pada Pengguna E-Commerce : Ancaman , Risiko , Strategi Kemanan (Literature Review)*. August.
<https://doi.org/10.31933/jimt.v4i5>
- Kurnia, N., Rahayu, Wendratama, E., Monggilo, Z. M. Z., Damayanti, A., Angendari, D. A. D., & Abisano, F. Q. (2022). *Penipuan Digital Di Indonesia*. Program Studi Magister Ilmu Komunikasi Fakultas Ilmu Sosial Dan Ilmu Politik Universitas Gadjah Mada.
- Maharan, A. P., Rivai, M., Sugianti, S., Fauzi, R. A. F. A., Azzahra, S., Ningsih, S., Lailiya, U., Adawiyah, R., Amalia, N. D. D., & Sudirman, S. (2021). Literasi Digital: Efektifitas Aplikasi Pedulilindungi Dalam Memberikan Informasi Pada Mahasiswa Fip Upi. *Indonesian Journal Of Adult And Community Education*, 3(2), 1–6.

- Maharani, A. C., & Purwanto, I. W. N. (2025). *Analisis Tanggung Jawab Bank Dalam Perlindungan Data Nasabah: Studi Kasus Perbankan Konvensional Dan Perbankan Digital*.
- Maulidiyah, M., Khoiriyah, E. Z., Putri, D. C., & Nurafini, F. (2024). *Analisis Faktor Yang Mempengaruhi Minat Masyarakat Lamongan Menjadi Nasabah Bank Syariah*. 7, 205–213.
- Megawati, I. A. P., & Kertiriasih, N. N. R. (2024). *Dampak Layanan Perbankan Digital Terhadap Kinerja Perbankan Di Indonesia*. 13(September), 1578–1591. <https://doi.org/10.34127/Jrlab.V13i3.1205>
- Modusaceh.Co. (2025). *Maraknya Penipuan Mengatasnamakan Bank Aceh, Nasabah Diminta Waspada*. Modusaceh.Co. https://modusaceh.co/news/maraknya-penipuan-mengatasnamakan-bank-aceh-nasabah-diminta-waspada/index.html#Google_Vignette
- Mulyadi, D., Mulyana, A., Carmenita, A., Utami, H. L., Aulia, K. A., Putri, M., & Alia, N. R. (2026). *Implementasi Kebijakan Pemerintah Terhadap Pencegahan Kebocoran Data Pribadi Dalam Pelayanan Publik Berbasis Digital*. 1, 1–15.
- Napitupulu, D. A. A., & Susanti, S. (2025). Pengaruh Pelatihan Peningkatan Kemampuan Literasi Digital Ibu Rumah Tangga Terhadap Pencegahan Penipuan Online Di Kelurahan Bunga Tanjung Kota Tanjung Balai. *Pendas: Jurnal Ilmiah Pendidikan Dasar*, 10(04), 250–261.

- Naufal, H. A. (2021). *Literasi Digital. Perspektif*, 1 (2), 195–202.
- Nisa, K., Purwono, Handayani, O. P., & Setiawan. (2025). *Peningkatan Literasi Digital: Edukasi Kejahatan Siber Dan Pinjaman Online Illegal Man 2 Cilacap*. 0(0).
<https://doi.org/10.35960/Pimas.V4i2.1831>
- Nupus, H., Kartini, A., & Desiana, L. (2025). Pengaruh Cyber Crime Dan Persepsi Keamanan Terhadap Tingkat Kepercayaan Pengguna Produk E-Banking (Survei Pada Pengguna E-Banking Bank Syariah Di Indonesia). *Jurnal Semesta Ilmu Manajemen Dan Ekonomi*, 1(3), 102–116.
- Nur'aini, R. J., & Simanjuntak, M. (2025). *Phishing Awareness And Security Concerns: Analyzing The Role Of Anti-Phishing Knowledge And Internet Experience In Online Banking Users*. 18(2), 121–133.
- Nur, F. (2025). *Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Penipuan Online Dengan Modus Social Engineering*. 5.
- Ojk. (2025). *Satgas Pasti Imbau Masyarakat Waspada Penipuan Menggunakan Artificial Intelligence*. Ojk.
<https://www.ojk.go.id/Id/Berita-Dan-Kegiatan/Info-Terkini/Pages/Satgas-Pasti-Imbau-Masyarakat-Waspada-Penipuan-Menggunakan-Ai.aspx>
- Permana, K. K., Eprianto, I., Fauzi, A., Minarny, T., & Fajriansyah, D. N. (2024). *Pengaruh Keamanan Data Pribadi Terhadap Kepercayaan Pengguna Di Era Transformasi Digital : Studi*

- Kasus Pada Aplikasi Mobile Banking*. 1(1), 37–46.
- Pradana, M. A. E., & Saragih, H. (2024). *Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap Gdpr Dan Akibat Hukumnya*. 4, 3412–3425.
- Prasetya, I. A., Hermanto, Sujatmiko, W., Wulandari, M., & Dzulqarnain, M. F. (2025). *Mewujudkan Kesadaran Keamanan Data Pribadi Pada Masyarakat Di Era Teknologi Informasi*. 6(September).
- Prasetyo, W. (2024). *Perlindungan Hukum Atas Data Pribadi Nasabah Dalam Penyelenggaraan Layanan Internet Banking Dihubungan Dengan Undang-Undang Nomor 10 Tahun 2988 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan*. 8(10), 34819–34825.
- Putra, F. A. N., Avanza, D. T., Asyifa, S. T., & Wahyuni, D. A. (2025). *Literasi Keamanan Data Pribadi Dan Privasi Digital*. 02(03), 2534–2536.
- Rahmah, A. T., & Fasa, M. I. (2024). *Pengaruh Transformasi Digital Dan Pengembangan Financial Technology (Fintech) Terhadap Inovasi Layanan Perbankan Syariah*. 2(3).
- Rahman, F. (2021). *Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia*.
- Reihandho, M. I., & Fajarwati, D. (2020). *Faktor-Faktor Yang*

Mempengaruhi Niat Penggunaan Perbankan Digital Di Indonesia Faktor-Faktor Yang Mempengaruhi Niat Penggunaan Perbankan Digital Di Indonesia.

- Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). *Computers & Security Which Factors Predict Susceptibility To Phishing ? An Empirical Study*. 136(September 2023). <https://doi.org/10.1016/j.cose.2023.103558>
- Rizal, C., Rosyidah, U. A., Yusnanto, T., Akbar, M. R., Hidayat, L., Setiawan, J., Ilham, A., Yunus, R., Wardhani, A. K., Rahajeng, E., Nay, F. A., Irawan, J. D., Muflihah, Y., & Asari, A. (2022). *Literasi Digital*.
- Rozi, F., & Samingan, A. (2024). *Syariah Kc Solo Dengan Kepuasan Sebagai Variabel*. 4(1), 95–104.
- Sahfitri, A., & Rosmalinda, R. (2024). *Penipuan Digital Melalui Tautan Phishing*. *Jurnal Dialektika Hukum*, 6(2), 92–107.
- Sembiring, E. R. 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 Sosial*, 5(4), 880–887.
- Serambinews.Com. (2025). *Marak Kasus Penipuan Online Di Banda Aceh Polresta Beri Warning Warga Untuk Tidak Terjebak*. Serambinews.Com. <https://aceh.tribunnews.com/2025/06/17/Marak-Kasus-Penipuan-Online-Di-Banda-Aceh-Polresta-Beri-Warning->

Warga-Untuk-Tidak-Terjebak

- Siagian, Y., Syah, A. Z., & Irawati, N. (2024). Peningkatan Kesadaran Dan Kewaspadaan Terhadap Ancaman Cybercrime Bagi Masyarakat Di Era Digital. *Jurnal Pengabdian Masyarakat Mitra Kreasi Cendekia (Mkc)*, 2(2), 164–169.
- Siahaan, P. G., Purba, N. R., Ritonga, N., & Silalahi, E. (2024). *Perlindungan Data Pribadi Terhadap Penanggulangan Tindakan Penipuan Online*. 9(1), 47–58.
- Sianturi, B. F. C. L., Alfian, R., Anendri, N. T., Fiyona, P., & Hidayat, M. F. (2024). *Perlindungan Hukum Terhadap Nasabah Bank Terkait Transaksi Digital Di Indonesia*. 1(4), 267–271.
- Sitompul, K. L. (2024). *Review : Analisis Faktor Yang Mempengaruhi Kemampuan Literasi Digital*.
- Suari, K. R. A., & Sarjana, I. M. (2023). *Menjaga Privasi Di Era Digital : Perlindungan Data Pribadi Di Indonesia*. 1, 132–146. <https://doi.org/10.38043/Jah.V6i1.4484>
- Sugiyono. (2023). *Metode Penelitian Kuantitatif, Kualitatif Dan R&D*. Alfabeta.
- Suail, A. A., Firdaus, Ramadhan, M. A., Putra, W. D., & Lestari, D. P. (2024). *Implementasi Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 11 Tahun 2020*. 3(4).
- Syafitri, N., & Agustin, G. (2023). *Social Engineering Swot Analysis In Government-Owned Commercial Banks And*

National Private Commercial Banks Department Of Development Economics , Faculty Of Economics And Business , Universitas Negeri Malang. 265–281.

- Syahrin, A., Mahlizar, & Sulfitra. (2025). Pengaruh Literasi Keuangan, Kemudahan, Dan Keamanan Terhadap Keputusan Bertransaksi Menggunakan Qris Pada Umkm Di Bsi Umkm Center Aceh: Pengaruh Literasi Keuangan, Kemudahan, Dan Keamanan Terhadap Keputusan Bertransaksi Menggunakan Qris Pada Umkm Di Bsi U. *Journal Islamic Economics Ad Diwan*, 4(2), 140–146.
- Tiffani, I. (2023). *Pengaruh Literasi Keuangan Dan Literasi Digital Terhadap Preferensi Bank Digital*. 22(1), 152–167.
- Wahib, P., Narotama, A. T., Rijki, N. M., Permana, F., Sagara, D., Azkhal, D. I., Anwar, M., & Juniawan, M. R. (2022). Sosialisasi Cyber Security Untuk Meningkatkan Literasi Digital. *Abdi Jurnal Publikasi*, 1(2), 64–68.
- Wahyuni, Y., Sartika, S. A., Marlina, L., & Siliwangi, U. (2025). *Analisis Maraknya Penipuan Bisnis Scam Di Aplikasi Telegram Pada Perspektif Islam*. 02(02).
- Wiguna, K. A., Gadjah, U., & Yogyakarta, M. (2023). *Analisis Kompetensi Literasi Digital Pada Guru Sekolah Menengah Atas*. 21–32.
- Winarto, S. R., & Bisma, R. (2021). *Studi Literatur : Analisis Persepsi Umkm Di Indonesia Terhadap Cyber Security Menggunakan Model Protection Motivation Theory (Pmt)*.

03, 20–28.

Yoviani, T., Dewi, A., & Ibnu, A. R. (2025). *Pengaruh Kemudahan, Keamanan Dan Literasi Digital Terhadap Minat Nasabah Menggunakan Aplikasi Muamalat Din*. 3(4), 324–336.



LAMPIRAN

Lampiran 1 Kuesioner Penelitian

Pengaruh Literasi Dan Keamanan Data Pribadi Terhadap Kewaspadaan terhadap Penipuan Digital Pada Nasabah Bank Aceh Syariah Di Kota Banda Aceh

Kepada Yth,
Bapak/Ibu/Saudara/I responden
Di tempat,

Dengan hormat, Saya mahasiswa program studi perbankan syariah Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Ar-Raniry Banda Aceh, yang sedang menyusun tugas akhir skripsi. Mengharapkan kesediaan dan partisipasi Bapak/Ibu/Saudara/I untuk mengisi kuesioner angket yang akan menjadi bantuan yang sangat berarti bagi saya.

Informasi yang diperoleh melalui kuesioner ini hanya digunakan untuk kepentingan penelitian dan tidak untuk kepentingan diluar itu, sehingga kerahasiaan jawaban Bapak/Ibu/Saudara/I akan tetap terjaga sesuai dengan aturan dan etika penelitian. Responden diharapkan membaca setiap pertanyaan dengan baik dan menjawab dengan lengkap. Tidak ada jawaban yang salah atau jawaban yang benar dalam pilihan Bapak/Ibu/Saudara/I yang penting adalah memilih jawaban sesuai pendapat yang dirasakan.

Demikianlah permohonan saya, atas ketersediaan Bapak/Ibu/Saudara/I dalam meluangkan waktu untuk mengisi dan menyatakan pendapat dalam penelitian ini saya ucapkan terimakasih banyak.

Hormat saya

Rifqi Aldian

NIM. 220603092



Kuesioner Penelitian

Petunjuk: Isilah kolom jawaban di bawah ini sesuai dengan identitas dan kondisi Anda yang sebenarnya.

No	Karakteristik Responden	Jawaban
1	Email	_____
2	Nama	_____
3	Jenis Kelamin	☐ Laki-laki ☐ Perempuan
4	Pekerjaan Utama	☐ ASN (PNS/PPPK) ☐ TNI/POLRI ☐ Pegawai Swasta ☐ Wiraswasta/Pengusaha ☐ Mahasiswa ☐ Pelajar ☐ Lainnya
5	Domisili	☐ Banda Raya ☐ Baiturrahman ☐ Jaya Baru ☐ Kuta Alam ☐ Kuta Raja ☐ Lueng Bata ☐ Meuraxa ☐ Syiah Kuala ☐ Ulee Kareng
6	Usia	☐ 17–25 tahun ☐ 26–35 tahun ☐ 36–45 tahun ☐ 46 tahun atau lebih
7	Pendidikan Terakhir	☐ SMA/SMK ☐ Diploma III ☐ S1/ D4

		☐ S2 ☐ S3
--	--	--

Petunjuk Pengisian: Berikan tanda centang (✓) pada kolom yang sesuai dengan kondisi Anda.

Keterangan:

- STS = Sangat Tidak Setuju
- TS = Tidak Setuju
- N = Netral
- S = Setuju
- SS = Sangat Setuju

No	Variabel	Indikator	Pernyataan	STS	TS	N	S	SS
1	Kewaspadaan terhadap Penipuan Digital (Y)	Kewaspadaan	Saya berhati-hati terhadap pesan atau telepon yang mengatasnamakan pihak bank.					
			Saya berhati-hati terhadap tautan dari pihak yang tidak dikenal.					
		Kesadaran	Saya menyadari bahwa layanan perbankan digital memiliki risiko penipuan.					
			Saya menyadari bahwa pelaku penipuan dapat mengatasnamakan pihak bank untuk memperoleh data pribadi nasabah.					

		Pengetahuan berbagai bentuk rekayasa sosial digital	Saya mengetahui berbagai modus penipuan digital, seperti <i>phishing</i> dan rekayasa sosial (<i>social engineering</i>).					
			Saya mengetahui bahwa pelaku penipuan digital dapat menyamar sebagai pihak bank atau lembaga keuangan resmi.					
2	Literasi Digital (X1)	Pencarian di Internet (<i>Internet Searching</i>)	Saya mampu menggunakan kata kunci yang tepat saat mencari informasi perbankan di internet.					
			Saya mampu menemukan informasi perbankan digital dari sumber yang relevan di internet.					
		Navigasi <i>Hypertext</i> (<i>Hypertextual Navigation</i>)	Saya mampu menggunakan tautan dan menu pada layanan perbankan digital dengan benar.					
			Saya mampu membedakan situs resmi dan situs palsu					

			layanan perbankan digital.					
		Evaluasi Konten Informasi (<i>Content Evaluation</i>)	Saya mampu membedakan informasi yang valid dan menyesatkan tentang layanan perbankan di internet.					
			Saya memverifikasi kebenaran informasi dari sumber terpercaya sebelum mempercayai konten yang beredar melalui media digital.					
		Penyusunan Pengetahuan (<i>Knowledge Assembly</i>)	Saya menggabungkan informasi dari berbagai sumber terpercaya untuk memahami risiko kejahatan digital.					
			Saya memanfaatkan informasi dari berbagai sumber untuk melakukan transaksi perbankan dengan lebih aman.					
3	Keamanan Data Pribadi (X2)	Kerahasiaan (<i>Confidentiality</i>)	Saya menjaga kerahasiaan PIN, kata sandi, dan kode OTP akun Action					

			Mobile saya.					
			Saya hanya memberikan data pribadi perbankan kepada pihak yang berwenang.					
		Integritas (Integrity)	Saya memastikan bahwa data pribadi yang saya berikan kepada layanan digital perbankan sudah akurat.					
			Saya bertanggung jawab untuk menjaga kerahasiaan data pribadi yang saya gunakan pada layanan perbankan digital.					
		Ketersediaan (Availability)	Saya memastikan informasi penting yang berkaitan dengan akun layanan perbankan digital tetap tersedia ketika saya membutuhkannya.					
			Saya memastikan akun layanan perbankan digital saya					

			dapat diakses kembali saat diperlukan melalui prosedur pemulihan akun yang tersedia.					
--	--	--	--	--	--	--	--	--



Lampiran 2 Hasil Tabulasi Kuesioner Responden

1. Variabel Literasi Digital (X1)

No. Responden	Literasi Digital							
	X1.1	X1.2	X1.3	X1.4	X1.5	X1.6	X1.7	X1.8
1	4	4	4	4	4	4	4	4
2	4	4	4	5	5	5	4	3
3	4	4	4	4	4	4	4	4
4	5	3	1	4	5	4	5	5
5	5	5	5	5	5	5	5	5
6	4	5	4	5	4	5	5	4
7	5	4	5	5	5	4	5	4
8	4	4	3	4	4	4	4	3
9	4	4	5	3	5	4	5	4
10	4	4	5	3	5	5	4	3
11	5	5	4	5	3	5	4	5
12	4	4	5	4	5	3	5	5
13	4	4	5	3	5	3	4	4
14	5	4	5	5	3	5	4	4
15	5	4	5	5	3	5	4	4
16	4	4	5	3	5	4	5	5
17	5	5	4	5	3	5	4	4
18	4	4	5	3	5	4	4	5
19	5	5	4	5	3	5	4	4
20	5	5	4	4	5	3	5	4
21	4	4	5	4	5	3	5	4
22	5	5	4	5	3	5	4	4
23	5	5	4	5	3	5	4	5
24	4	4	5	3	5	4	5	5
25	5	5	4	5	3	5	4	4
26	5	5	4	5	3	5	4	4
27	5	5	4	5	3	5	4	4
28	4	5	4	3	4	5	5	3
29	5	4	5	3	5	3	4	5
30	5	4	4	3	4	5	4	5
31	5	3	4	5	4	5	3	4
32	5	4	3	4	5	4	3	5
33	5	4	5	3	4	4	5	4

34	5	4	3	4	5	4	3	5
35	5	4	5	4	5	3	5	4
36	5	5	4	5	3	5	4	4
37	4	3	5	5	4	5	4	3
38	5	4	4	3	5	5	4	4
39	2	4	3	2	4	4	5	2
40	2	3	1	2	2	4	5	2
41	4	5	3	5	4	4	5	3
42	5	3	4	5	4	5	5	3
43	4	5	5	3	4	4	5	5
44	4	4	3	4	5	5	4	5
45	5	4	3	4	5	4	3	4
46	4	3	5	4	4	3	5	4
47	5	4	5	3	4	5	4	5
48	4	4	5	4	3	4	5	4
49	5	4	3	5	4	3	5	4
50	5	4	5	3	4	5	4	5
51	4	3	5	5	4	4	3	5
52	5	4	5	3	4	5	4	5
53	4	5	3	4	5	4	5	4
54	5	5	4	5	4	4	5	4
55	5	4	5	3	4	5	3	4
56	5	5	4	5	4	4	5	4
57	2	2	1	3	2	2	1	2
58	5	4	5	5	3	5	4	5
59	4	4	5	3	5	4	5	5
60	4	4	5	4	5	5	3	5
61	4	4	5	4	5	5	4	5
62	5	5	4	5	4	4	3	4
63	4	5	3	5	5	4	4	5
64	5	5	5	3	4	5	3	4
65	4	4	5	4	5	5	4	5
66	5	4	5	5	4	5	4	4
67	5	4	4	5	3	4	5	5
68	4	5	3	4	4	4	5	5
69	4	4	5	3	5	5	4	3
70	4	4	5	4	5	5	4	5
71	4	5	3	5	4	4	5	4

72	2	1	1	4	2	3	4	4
73	5	4	4	3	5	4	5	5
74	5	5	4	5	3	5	4	4
75	4	3	5	5	4	5	4	3
76	4	3	4	5	5	4	5	3
77	5	4	5	5	3	4	4	5
78	5	4	3	5	4	3	5	4
79	5	4	4	3	5	4	3	4
80	5	4	3	5	4	4	5	5
81	5	4	5	3	4	5	4	5
82	5	4	5	3	5	4	4	5
83	5	4	4	5	3	5	4	4
84	4	5	5	3	5	5	4	5
85	4	5	4	5	3	4	5	5
86	5	5	4	5	3	3	5	3
87	4	5	4	5	5	3	5	4
88	4	5	3	5	4	5	5	4
89	4	5	4	5	5	4	5	4
90	5	4	5	3	5	4	5	5
91	4	5	3	5	4	5	5	3
92	4	5	4	5	5	5	4	5
93	5	4	5	5	4	5	4	4
94	4	5	4	5	5	5	4	4
95	4	5	4	4	2	4	5	4
96	4	5	4	5	5	4	5	4
97	4	5	3	5	4	5	5	4
98	5	4	5	5	4	5	4	3
99	4	4	5	4	5	5	4	5
100	5	4	5	5	4	5	4	5
101	4	4	5	4	5	4	4	4
102	4	5	3	5	4	4	5	4
103	4	5	3	5	5	4	4	5
104	4	5	4	3	5	5	4	5
105	3	5	5	4	5	4	5	5
106	4	4	5	3	4	5	5	4
107	4	4	5	3	5	3	4	5
108	4	4	5	4	5	5	4	5
109	5	3	4	5	5	4	4	5

110	4	5	4	3	5	5	4	4
111	5	4	5	5	3	5	4	5
112	4	5	4	5	4	5	5	4
113	4	5	4	5	5	3	4	5
114	4	5	4	5	5	3	4	5
115	4	5	4	5	5	4	3	5
116	5	3	4	4	5	4	5	5
117	5	4	5	5	4	5	3	4
118	3	4	5	4	5	5	4	5
119	4	5	5	5	5	4	5	4
120	4	5	5	5	4	4	5	4
121	4	3	5	5	4	4	5	5
122	4	4	5	3	4	5	5	4
123	1	1	2	5	4	2	2	3
124	4	5	4	5	4	5	3	4
125	4	5	5	4	3	5	5	4
126	4	5	5	4	5	3	5	4
127	4	4	2	5	4	4	3	1
128	5	3	4	4	5	5	4	4
129	3	5	4	5	5	4	3	5
130	4	4	5	5	4	3	5	4
131	3	5	4	4	5	5	4	4
132	4	5	5	3	4	5	5	4
133	3	5	5	4	5	5	4	5
134	5	4	3	5	5	5	4	4
135	5	4	4	5	5	4	4	4
136	4	4	5	4	5	5	5	4
137	5	5	4	4	3	4	5	4
138	5	3	4	4	5	5	5	3
139	5	4	5	5	3	5	4	4
140	4	5	5	5	4	4	5	5
141	5	5	4	5	3	5	4	4
142	4	4	5	5	4	4	3	4
143	5	4	5	5	3	5	4	4
144	5	5	3	5	4	5	5	4
145	5	4	5	5	3	5	4	5
146	4	5	4	4	5	4	5	3
147	5	5	4	5	3	5	4	4

148	5	4	5	3	5	5	4	4
149	5	4	4	5	3	5	4	5
150	4	5	5	5	3	5	4	4
151	4	5	4	5	3	4	5	4
152	4	5	4	5	5	3	5	4
153	4	5	4	5	5	4	5	3
154	4	5	4	5	5	4	5	4
155	5	4	5	5	3	4	5	4
156	4	5	4	4	5	3	5	4
157	4	2	4	5	5	2	1	2
158	4	4	5	4	4	3	5	5
159	5	3	5	4	5	4	5	4
160	4	5	5	3	4	4	4	5
161	5	3	4	5	5	4	4	5
162	4	5	5	4	3	5	5	5
163	5	5	3	4	5	4	5	4
164	5	4	5	3	4	5	4	5
165	4	5	5	4	3	5	4	4
166	5	4	5	4	3	4	5	4
167	3	5	5	4	4	5	5	4
168	5	4	5	4	5	3	4	5
169	4	5	5	3	5	4	4	5
170	5	4	5	3	4	5	4	5
171	4	5	5	3	5	5	4	4
172	4	5	5	3	5	4	4	5
173	5	5	4	5	3	5	4	4
174	5	4	5	4	3	4	5	4
175	5	4	5	3	5	4	5	4
176	4	5	4	5	5	3	5	4
177	5	5	4	5	3	5	4	4
178	4	4	5	3	5	4	2	2
179	4	5	4	5	3	5	4	5
180	5	4	5	3	5	4	5	4
181	5	4	5	3	5	4	5	4
182	5	4	5	3	5	4	5	4
183	5	4	5	3	5	4	5	4
184	5	4	5	3	5	4	5	4
185	4	5	4	5	3	5	4	5

186	5	4	5	3	5	4	5	4
187	4	4	5	4	5	4	4	5
188	4	5	4	4	5	4	5	4
189	4	4	5	4	5	4	4	5
190	4	5	4	4	5	4	5	4
191	4	5	4	5	3	5	5	4
192	4	5	4	4	5	4	5	4
193	4	5	4	4	5	4	5	4
194	4	5	4	4	5	4	4	5
195	4	4	5	4	5	4	4	5
196	4	3	5	5	4	4	5	5
197	5	4	5	3	5	4	2	4
198	4	4	5	4	5	4	4	5
199	4	5	5	4	5	3	5	4
200	4	5	4	4	5	4	5	4
201	4	4	5	3	5	4	4	5
202	4	5	3	5	4	4	5	5
203	4	5	4	5	3	5	4	5
204	5	4	5	3	4	5	4	5
205	5	4	5	3	4	5	4	4
206	5	4	5	4	3	4	5	4
207	4	5	5	4	4	5	5	4
208	4	5	5	3	5	4	3	5
209	5	4	5	3	5	4	5	4
210	5	5	4	4	5	4	4	5
211	5	4	5	3	5	4	5	4
212	5	5	4	4	5	4	5	5
213	4	5	4	5	3	5	4	5
214	4	5	4	4	5	5	4	4
215	5	4	5	3	5	4	5	4
216	5	3	5	5	4	4	5	4
217	4	5	4	5	3	5	4	5
218	5	5	4	4	5	4	5	5
219	4	5	3	4	5	5	4	5
220	5	5	4	5	4	5	4	4
221	5	3	5	5	4	5	5	4
222	5	4	5	3	5	4	5	4
223	4	5	4	5	5	3	4	5

224	4	5	4	5	5	4	3	4
225	5	5	4	3	5	4	5	4
226	4	4	5	4	5	4	4	5
227	5	4	5	5	4	5	3	4
228	5	4	5	5	4	5	3	4
229	4	5	4	5	5	3	4	4
230	4	5	3	4	4	5	4	5
231	4	4	5	4	5	4	4	5
232	5	4	5	3	4	5	4	5
233	5	4	5	3	4	5	5	4
234	4	4	5	4	5	4	4	5
235	5	4	5	3	4	5	4	5
236	4	5	4	4	2	3	4	2
237	4	4	5	4	5	4	4	5
238	4	4	5	4	5	4	4	5
239	4	5	4	5	3	4	5	4
240	5	4	5	3	5	4	5	4
241	5	4	5	3	4	5	4	4
242	4	4	5	4	5	4	5	5
243	5	4	4	5	4	3	4	5
244	4	5	4	4	5	4	5	4
245	4	5	4	4	5	4	4	5
246	4	5	4	4	5	4	5	4
247	5	4	5	5	4	4	5	5
248	2	2	1	2	1	2	2	1
249	4	5	5	3	4	4	5	5
250	5	4	5	5	4	4	5	5
251	5	4	4	5	5	4	5	4
252	5	4	4	5	5	4	5	4
253	4	5	4	4	5	5	4	4
254	5	5	4	5	5	4	5	5
255	5	4	4	5	5	4	5	5
256	5	4	4	5	3	5	5	4
257	4	5	5	4	5	3	5	4
258	4	5	5	4	5	3	4	4
259	4	5	5	3	5	4	5	4
260	4	5	5	4	4	5	3	4
261	2	1	3	2	4	5	4	2

262	2	3	1	2	4	5	3	1
263	4	5	4	3	5	4	5	5
264	4	3	4	5	4	5	5	4
265	4	5	3	4	5	5	4	5
266	5	4	5	3	1	2	4	4
267	5	4	3	5	4	5	4	5
268	4	5	4	5	3	4	5	5
269	4	5	4	4	5	3	4	5
270	4	3	4	5	4	5	5	4
271	4	5	4	4	5	4	5	3
272	4	5	4	5	5	3	4	5
273	4	5	5	4	3	4	5	4
274	5	4	3	5	4	4	5	3
275	5	4	3	5	4	3	4	5
276	4	5	4	3	5	4	4	5
277	4	5	3	4	5	4	4	3
278	4	4	5	4	5	4	4	5
279	4	5	3	5	4	4	3	4
280	4	5	4	3	4	4	5	3
281	4	4	5	4	5	4	4	5
282	4	4	5	4	5	4	4	5
283	4	4	5	5	4	4	5	4
284	5	4	5	4	5	4	5	4
285	4	4	5	2	4	5	4	4
286	4	4	5	4	5	4	4	5
287	4	4	5	4	5	4	4	5
288	3	4	3	1	2	3	4	4
289	2	5	2	3	5	1	5	2
290	2	4	2	4	4	2	3	4
291	2	5	4	4	2	3	5	3
292	5	3	2	1	4	3	3	3
293	4	2	3	1	4	4	3	3
294	4	2	4	3	4	5	5	4
295	5	3	5	2	4	4	2	4
296	4	4	2	5	2	4	1	4
297	5	3	3	2	3	4	2	5
298	5	3	3	3	4	3	3	1
299	5	3	4	1	3	4	3	4

300	4	4	3	3	5	4	3	3
301	5	3	4	2	2	4	1	3
302	5	2	4	1	4	2	3	4
303	5	2	3	3	2	4	2	4
304	5	3	3	2	5	5	3	2
305	5	2	3	2	5	4	2	3
306	4	2	3	1	2	4	2	4
307	5	4	5	2	4	4	2	3
308	3	5	2	1	5	2	1	3
309	4	3	4	2	5	3	1	3
310	3	2	3	2	2	3	1	5
311	4	3	4	3	3	4	3	4
312	4	2	3	2	5	2	4	5
313	5	3	4	2	2	4	3	4
314	4	3	4	2	3	4	1	4
315	5	2	4	2	2	5	2	5
316	4	3	3	2	2	3	5	4
317	3	3	3	2	2	3	2	5
318	5	2	5	2	4	2	4	3
319	4	3	5	2	2	2	2	4
320	5	3	4	2	2	3	4	4
321	4	2	4	2	2	4	1	5
322	4	2	3	3	2	5	3	3
323	4	3	3	2	2	3	2	4
324	4	3	3	4	1	4	2	5
325	5	2	3	2	5	4	2	5
326	4	3	3	2	4	4	1	3
327	5	2	3	2	3	4	5	4
328	5	2	4	1	4	5	5	5
329	4	2	3	2	1	3	3	4
330	3	2	3	1	2	4	2	5
331	4	1	3	1	4	4	2	4
332	4	2	2	2	5	4	2	4
333	5	2	4	1	4	4	2	4
334	3	2	4	2	3	3	5	2
335	4	3	3	2	3	3	3	3
336	4	3	4	2	3	3	4	4
337	5	2	3	2	3	4	2	3

338	4	4	3	3	5	4	1	3
339	4	3	2	2	4	4	2	3
340	4	2	1	2	4	4	5	3
341	5	3	3	1	2	3	5	3
342	4	5	3	4	3	3	1	3
343	4	3	3	3	3	4	2	2
344	4	5	3	3	4	4	3	3
345	4	4	3	2	4	4	2	3
346	4	3	3	1	4	2	2	4
347	3	3	3	1	4	2	5	3
348	4	4	3	4	3	4	3	5
349	4	3	3	5	4	3	4	5
350	4	5	3	4	5	4	4	4
351	5	4	5	3	5	4	4	5
352	5	4	5	3	5	5	3	5
353	4	4	5	3	5	4	5	5
354	4	4	5	3	5	4	5	5
355	4	4	5	3	5	4	4	5
356	5	4	3	5	4	5	4	4
357	4	5	4	4	3	4	5	4
358	4	5	4	4	5	4	3	4
359	4	3	4	5	4	4	5	4
360	4	5	4	5	3	4	5	5
361	4	4	5	4	5	5	3	4
362	4	4	5	4	5	5	4	5
363	5	5	4	5	4	4	5	4
364	4	4	5	3	4	4	5	4
365	4	4	5	4	5	5	3	4
366	3	5	4	5	3	5	4	5
367	4	3	5	4	5	3	5	4
368	5	3	5	4	5	4	5	3
369	3	5	4	5	4	5	3	5
370	4	3	5	4	5	3	5	4
371	5	4	3	5	4	3	4	5
372	4	5	5	3	5	4	4	5
373	5	4	4	3	4	4	5	4
374	4	5	5	4	4	5	3	5
375	5	4	3	5	4	4	4	5

376	5	4	3	5	5	4	4	5
377	4	4	3	4	5	4	5	3
378	5	4	4	5	5	3	5	5
379	4	5	4	5	3	5	4	3
380	5	4	5	5	4	5	4	5
381	5	4	5	3	5	5	4	5
382	5	4	3	5	5	4	5	4
383	5	4	3	4	5	4	5	5
384	5	5	4	5	3	5	4	5

2. Variabel Keamanan Data Pribadi (X2)

No. Responde n	Keamanan Data Pribadi					
	X2.1	X2.2	X2.3	X2.4	X2.5	X2.6
1	5	5	5	4	4	4
2	5	3	5	3	5	4
3	4	4	4	4	4	4
4	5	4	5	5	5	4
5	5	5	5	5	5	5
6	4	5	4	4	4	4
7	4	5	5	5	4	5
8	5	4	4	4	4	4
9	4	4	5	5	4	4
10	5	4	5	5	5	4
11	4	4	5	3	5	4
12	4	5	4	4	5	3
13	5	4	5	5	4	4
14	5	4	5	5	4	5
15	5	4	5	5	4	4
16	4	4	5	3	5	4
17	5	4	4	5	4	5
18	3	5	4	4	5	4
19	5	4	5	5	4	5
20	5	5	4	5	3	5
21	5	5	4	5	4	5
22	5	5	4	5	4	3
23	4	4	5	3	5	4

24	4	5	4	4	5	3
25	5	4	5	5	3	5
26	5	4	5	5	3	5
27	5	4	5	3	4	4
28	5	4	4	4	5	5
29	4	5	3	5	4	4
30	3	4	5	4	4	3
31	5	4	3	5	4	5
32	5	3	5	4	5	3
33	4	3	5	4	3	5
34	3	4	5	4	3	5
35	5	4	5	3	4	5
36	5	3	5	5	5	4
37	5	5	4	5	3	4
38	5	3	5	3	5	5
39	1	2	3	1	2	1
40	2	3	1	2	5	2
41	5	5	4	4	3	4
42	2	3	1	2	3	1
43	5	4	4	3	5	4
44	5	3	5	5	5	3
45	4	3	5	4	3	4
46	5	4	3	5	4	3
47	4	5	3	4	5	4
48	4	5	4	4	5	5
49	5	4	3	5	4	3
50	5	4	5	3	5	4
51	4	4	3	5	4	5
52	4	5	3	4	5	3
53	5	4	5	3	5	4
54	5	4	5	4	4	5
55	5	4	5	4	3	4
56	3	5	4	5	4	4
57	3	2	2	1	2	1
58	5	5	4	5	4	4
59	4	4	5	4	5	3
60	4	4	5	4	5	5
61	3	5	4	4	5	4

62	5	4	5	5	4	5
63	3	5	4	5	5	4
64	5	4	4	5	3	4
65	3	5	4	5	5	4
66	3	5	4	5	5	4
67	4	5	3	5	4	4
68	4	4	5	3	5	4
69	5	3	5	4	5	3
70	3	5	4	5	5	4
71	5	3	5	4	4	5
72	2	2	4	1	3	2
73	4	3	5	4	4	5
74	5	4	5	3	5	4
75	5	5	4	5	3	4
76	5	4	3	5	5	4
77	4	4	5	3	4	5
78	5	3	4	4	5	3
79	4	5	3	4	4	5
80	4	3	5	4	3	5
81	4	5	3	4	5	4
82	4	3	4	5	4	5
83	5	4	3	5	5	3
84	5	4	5	4	3	5
85	4	5	4	5	4	4
86	5	5	4	5	4	4
87	4	5	4	4	5	4
88	5	4	5	3	4	5
89	5	3	5	4	5	4
90	4	5	3	4	5	5
91	5	5	4	5	4	1
92	4	5	4	5	5	3
93	4	3	5	4	5	5
94	5	3	5	4	5	5
95	5	5	4	5	4	4
96	4	3	5	4	5	5
97	3	5	4	4	5	4
98	4	5	4	5	5	4
99	5	4	5	5	4	4

100	4	4	5	3	5	4
101	5	4	3	5	4	4
102	3	5	5	4	5	4
103	3	4	4	5	4	5
104	4	5	5	3	5	5
105	3	4	5	4	5	5
106	3	5	4	5	5	4
107	3	5	4	4	3	5
108	4	4	5	5	5	4
109	5	5	5	4	4	5
110	5	3	4	5	5	4
111	4	5	4	5	5	4
112	4	3	4	5	4	5
113	4	5	4	5	5	4
114	4	5	4	4	5	3
115	4	5	4	5	5	3
116	4	5	4	5	5	4
117	4	5	4	4	5	4
118	4	5	4	4	5	4
119	4	5	4	5	5	5
120	4	5	5	4	4	5
121	5	4	4	5	5	3
122	4	5	5	3	5	4
123	4	1	4	2	3	5
124	3	5	4	5	4	5
125	5	5	4	5	3	4
126	5	5	4	5	4	3
127	4	5	5	4	3	4
128	3	5	4	5	4	4
129	4	5	5	4	3	4
130	5	3	5	5	4	4
131	5	3	5	5	4	5
132	5	4	4	5	5	4
133	4	5	5	3	5	4
134	5	3	5	5	4	4
135	5	5	4	5	4	4
136	4	3	4	3	5	5
137	4	3	4	5	5	4

138	4	5	4	3	4	4
139	5	3	5	5	4	5
140	5	4	4	5	5	5
141	5	4	5	5	3	5
142	5	3	4	4	5	3
143	5	3	5	4	4	5
144	5	4	5	5	3	4
145	4	4	3	5	4	5
146	4	5	4	4	5	4
147	5	4	5	5	4	5
148	3	5	4	5	4	4
149	4	4	5	4	3	4
150	4	5	4	3	5	4
151	5	4	5	5	3	4
152	5	4	5	4	4	5
153	4	5	4	5	5	4
154	5	4	3	5	4	5
155	5	4	5	5	4	5
156	5	4	5	5	4	5
157	4	5	4	4	5	4
158	4	5	3	5	5	4
159	5	4	5	5	3	5
160	3	5	5	4	5	3
161	4	5	4	3	5	5
162	4	5	4	3	5	5
163	5	4	5	3	4	4
164	5	4	5	3	5	3
165	5	5	4	3	5	4
166	5	4	5	3	4	5
167	5	3	5	5	4	4
168	4	5	3	4	5	4
169	5	5	3	5	5	4
170	5	4	5	4	5	4
171	5	4	4	5	3	5
172	4	5	3	5	5	4
173	5	4	4	5	3	5
174	5	3	5	4	5	4
175	5	3	5	4	5	4

176	4	5	3	5	4	4
177	5	4	5	5	3	5
178	4	5	4	4	5	4
179	5	4	5	3	5	4
180	4	5	3	5	4	5
181	4	5	3	5	4	5
182	4	5	3	5	4	5
183	4	5	3	5	4	5
184	5	4	5	4	5	4
185	5	4	5	3	5	4
186	4	5	3	5	4	5
187	4	5	4	4	5	4
188	4	4	5	4	5	4
189	4	5	4	4	5	4
190	4	4	5	4	5	4
191	5	4	4	5	3	4
192	4	4	5	4	5	4
193	4	4	5	4	5	4
194	4	4	5	4	5	4
195	4	5	4	4	5	4
196	4	5	3	5	5	4
197	5	3	5	4	4	2
198	4	4	5	4	5	4
199	5	5	4	5	5	3
200	5	4	4	5	4	5
201	4	4	5	5	3	5
202	4	5	3	5	5	4
203	5	4	5	3	5	4
204	4	5	4	5	3	4
205	5	4	5	4	3	5
206	5	3	4	5	4	5
207	5	5	4	5	4	4
208	4	5	5	4	4	5
209	4	5	3	5	4	5
210	4	4	5	3	5	5
211	4	5	3	5	4	5
212	4	4	5	5	4	4
213	5	4	5	3	5	4

214	5	4	4	5	5	4
215	4	5	3	5	4	5
216	5	5	4	4	5	4
217	5	4	5	3	5	4
218	4	5	4	4	5	5
219	4	5	3	5	5	4
220	5	5	4	5	4	4
221	5	5	4	4	5	4
222	4	5	3	5	4	5
223	4	5	3	4	4	5
224	5	4	5	4	4	5
225	5	4	5	5	4	5
226	4	5	4	4	5	4
227	5	4	5	4	3	4
228	5	4	5	5	3	4
229	5	4	5	5	4	5
230	4	5	4	4	5	4
231	4	4	5	4	5	4
232	5	4	5	3	4	5
233	5	3	4	5	4	5
234	4	5	4	4	5	4
235	4	5	5	4	3	4
236	4	4	5	5	4	5
237	4	4	5	4	5	4
238	4	4	5	4	4	5
239	5	4	5	4	3	4
240	4	5	3	5	4	5
241	4	3	5	4	5	4
242	4	4	5	5	4	5
243	4	5	3	3	4	5
244	4	4	5	4	5	4
245	4	5	4	4	5	4
246	5	4	5	3	5	4
247	3	5	5	4	5	5
248	2	2	1	2	1	2
249	5	3	4	5	5	4
250	4	5	5	4	4	5
251	4	5	5	4	4	5

252	4	5	5	4	5	5
253	5	5	4	4	5	4
254	5	4	5	5	4	4
255	4	4	5	5	4	4
256	5	3	5	5	4	4
257	5	5	4	5	3	5
258	5	4	4	5	5	3
259	5	5	4	5	3	4
260	3	5	5	4	4	5
261	1	2	2	1	2	4
262	2	4	5	3	2	1
263	4	5	4	5	5	3
264	5	3	5	4	5	4
265	4	5	4	3	5	4
266	5	4	2	4	5	4
267	3	5	4	5	5	4
268	4	5	3	4	4	5
269	4	5	4	4	5	4
270	5	4	5	5	4	5
271	4	5	4	5	5	3
272	4	3	4	4	5	4
273	5	4	4	3	5	5
274	4	5	4	3	4	5
275	4	5	5	3	5	4
276	3	4	5	4	3	4
277	5	3	4	5	4	3
278	4	4	5	4	5	4
279	5	5	4	3	4	4
280	5	4	4	4	5	3
281	4	5	4	4	5	4
282	4	5	4	4	5	4
283	5	4	4	5	4	5
284	5	4	5	4	5	4
285	5	4	4	5	4	5
286	4	5	4	4	5	4
287	4	5	4	4	5	4
288	4	4	1	2	4	4
289	2	5	3	2	4	4

290	2	5	2	2	4	4
291	2	4	2	4	4	3
292	4	3	4	1	3	3
293	4	3	4	1	3	4
294	5	3	4	2	3	4
295	4	3	3	2	3	5
296	5	3	4	3	2	5
297	3	1	3	2	3	4
298	4	2	3	2	2	4
299	5	3	3	2	2	4
300	4	4	4	3	2	4
301	4	3	5	2	2	4
302	3	3	4	2	1	3
303	5	3	4	2	2	4
304	5	3	4	3	2	4
305	5	3	3	2	1	3
306	5	2	3	2	3	5
307	4	3	4	1	3	4
308	4	2	2	5	4	3
309	3	3	3	2	2	3
310	4	3	3	1	1	3
311	4	3	3	4	5	3
312	4	4	4	2	2	4
313	4	3	5	2	2	3
314	4	3	4	1	3	4
315	5	3	4	2	2	4
316	4	3	4	2	2	3
317	3	2	4	2	2	4
318	5	3	4	4	4	4
319	4	4	4	2	2	3
320	5	3	4	5	2	3
321	5	3	4	1	2	3
322	4	3	4	2	2	4
323	4	3	4	2	1	4
324	4	3	3	2	2	4
325	4	3	4	2	2	4
326	4	3	5	2	3	4
327	4	3	3	2	3	3

328	4	3	4	2	4	2
329	4	3	3	1	2	4
330	3	3	3	1	2	4
331	4	3	3	1	2	4
332	5	3	3	4	3	4
333	5	3	3	1	3	3
334	4	3	4	1	3	4
335	4	3	3	1	2	3
336	5	3	4	1	2	3
337	4	2	3	1	1	4
338	3	4	5	2	4	2
339	4	5	4	2	4	3
340	4	3	1	1	3	3
341	5	5	3	3	3	3
342	1	3	2	4	3	2
343	3	4	3	5	4	2
344	4	4	3	3	1	2
345	3	4	4	2	5	4
346	4	4	3	2	4	3
347	3	3	3	2	5	3
348	5	5	5	4	4	4
349	5	5	5	4	3	4
350	5	5	4	4	5	5
351	4	5	3	5	4	4
352	4	5	3	5	4	3
353	4	4	5	3	5	4
354	4	5	3	5	5	4
355	4	4	5	3	5	4
356	5	4	5	4	4	3
357	5	4	5	4	3	4
358	5	4	5	5	4	3
359	5	4	5	4	3	5
360	4	5	4	5	5	4
361	5	4	5	5	4	5
362	3	5	5	4	5	4
363	5	3	4	5	4	4
364	3	4	4	5	4	5
365	5	4	4	3	5	4

366	5	3	4	3	5	4
367	5	3	5	4	5	3
368	4	5	5	4	5	3
369	4	5	3	5	4	5
370	4	3	5	4	5	3
371	5	5	4	3	4	4
372	4	5	5	3	5	4
373	5	4	4	3	3	4
374	4	5	5	4	4	5
375	5	3	3	4	4	5
376	4	5	5	3	5	4
377	5	4	4	5	4	3
378	4	4	5	3	5	4
379	5	4	5	4	3	4
380	4	5	4	3	5	4
381	4	5	3	5	5	4
382	4	5	5	4	5	3
383	4	5	4	4	5	4
384	4	4	5	4	5	3

3. Variabel Kewaspadaan Terhadap Penipuan Digital (Y)

No. Responden	Kewaspadaan terhadap penipuan (Y1)					
	Y1.1	Y1.2	Y1.3	Y1.4	Y1.5	Y1.6
1	5	5	4	5	4	4
2	5	5	4	5	5	5
3	4	4	4	4	4	4
4	5	5	5	5	4	5
5	5	5	5	5	5	5
6	5	5	4	5	5	4
7	5	5	4	4	4	5
8	5	5	3	4	3	3
9	5	5	4	4	4	4
10	3	5	4	4	5	4
11	5	5	4	4	5	3
12	5	4	5	5	4	5
13	5	4	5	5	4	5
14	3	5	4	4	5	4

15	3	5	4	4	5	4
16	5	5	4	5	3	5
17	4	5	4	4	5	5
18	5	5	4	5	3	5
19	3	5	4	5	5	4
20	4	4	5	4	5	5
21	3	5	4	4	4	5
22	5	5	4	5	3	5
23	5	4	5	4	5	4
24	5	4	5	5	4	5
25	4	5	5	4	5	3
26	4	4	5	4	5	5
27	5	4	5	4	4	3
28	4	3	5	4	5	4
29	3	5	4	5	5	3
30	5	4	5	5	3	4
31	3	5	4	4	5	3
32	4	5	5	3	5	4
33	5	4	5	3	5	4
34	4	5	5	3	5	4
35	4	5	3	4	5	4
36	5	5	4	5	3	4
37	5	5	4	5	3	5
38	4	3	5	4	5	5
39	1	2	2	3	1	1
40	3	1	3	5	2	2
41	5	4	4	5	4	5
42	4	5	5	3	5	4
43	4	5	3	4	5	4
44	4	5	4	5	5	4
45	3	4	5	4	5	3
46	5	4	5	3	5	4
47	5	4	5	3	4	5
48	3	5	5	4	5	4
49	5	5	4	3	5	3
50	5	4	3	4	5	4
51	3	4	5	4	3	4
52	4	5	3	4	5	4

53	5	5	3	4	5	4
54	3	5	4	5	5	4
55	5	3	4	5	3	4
56	4	4	5	4	5	5
57	1	2	1	2	2	1
58	3	5	4	5	5	4
59	5	4	5	5	4	5
60	3	4	4	5	4	5
61	5	5	4	5	4	4
62	3	5	5	4	5	4
63	3	5	5	3	4	5
64	5	4	5	3	4	5
65	4	4	5	3	5	4
66	4	4	5	3	5	4
67	5	4	4	5	5	3
68	4	5	5	4	3	5
69	4	5	5	5	4	4
70	4	3	5	4	5	5
71	4	3	5	5	4	5
72	5	2	3	1	1	2
73	4	5	4	3	5	4
74	5	5	3	5	4	4
75	5	5	4	5	3	4
76	5	4	5	3	5	4
77	3	4	4	5	4	5
78	3	5	4	5	4	5
79	3	5	4	4	3	5
80	4	4	3	5	4	5
81	5	5	4	3	5	4
82	3	5	4	4	3	5
83	5	5	4	3	5	4
84	4	5	4	5	3	5
85	5	4	5	5	4	5
86	5	4	5	5	4	3
87	4	5	4	5	5	4
88	4	5	4	5	3	4
89	4	4	5	4	5	5
90	4	5	4	5	5	4

91	4	5	5	4	5	4
92	4	5	4	5	5	5
93	4	5	4	5	5	4
94	4	5	3	5	4	5
95	4	5	4	4	3	1
96	4	4	5	4	3	4
97	3	5	4	5	5	4
98	4	4	5	4	5	3
99	4	4	5	4	5	3
100	4	4	5	3	4	4
101	5	3	5	4	4	5
102	5	4	3	4	5	4
103	4	3	5	5	4	5
104	4	5	5	4	3	5
105	4	4	3	3	5	4
106	4	4	5	4	5	4
107	4	5	4	4	5	5
108	4	5	5	4	4	3
109	4	4	5	3	5	4
110	5	4	4	5	5	4
111	5	4	5	3	4	5
112	4	5	4	5	5	4
113	4	5	3	5	4	5
114	4	5	4	5	4	4
115	4	5	4	5	4	4
116	4	3	4	5	4	5
117	5	3	4	5	4	4
118	4	5	4	4	5	2
119	5	5	4	4	5	4
120	5	4	5	5	5	4
121	5	5	4	4	5	5
122	5	3	5	4	4	5
123	2	2	1	4	2	1
124	4	5	5	3	4	4
125	5	5	4	5	3	4
126	5	4	5	5	5	4
127	5	5	4	2	4	3
128	5	3	4	5	5	4

129	5	4	4	3	4	5
130	5	4	5	5	4	5
131	4	5	5	4	5	5
132	5	3	5	5	4	4
133	5	4	4	5	5	5
134	5	4	3	4	5	4
135	5	3	4	4	3	5
136	4	4	5	5	4	5
137	5	3	4	5	5	4
138	5	4	4	5	3	4
139	4	4	5	5	4	5
140	4	4	5	5	4	5
141	4	4	5	5	4	5
142	5	5	5	4	4	3
143	4	5	3	5	4	5
144	5	4	4	5	5	4
145	4	5	4	3	5	4
146	5	4	4	5	4	5
147	3	5	4	4	5	4
148	5	4	5	3	4	4
149	5	5	4	5	4	4
150	4	5	3	5	5	4
151	4	5	4	4	5	4
152	4	5	3	5	4	5
153	4	5	4	5	5	4
154	4	5	4	5	5	4
155	4	3	5	4	5	5
156	5	4	3	5	4	5
157	2	3	2	1	2	1
158	3	5	4	4	5	5
159	5	5	4	5	5	4
160	4	5	5	4	5	5
161	4	5	4	3	5	3
162	4	4	3	5	4	5
163	5	4	5	3	4	5
164	5	3	4	5	4	5
165	4	3	5	5	4	5
166	4	5	5	3	5	4

167	5	4	4	5	3	4
168	4	5	3	5	4	5
169	5	3	4	4	5	4
170	3	5	4	5	4	5
171	4	4	5	5	3	4
172	5	5	4	4	5	4
173	4	5	5	4	4	5
174	5	4	5	3	4	5
175	5	3	4	5	4	5
176	5	5	4	5	5	4
177	4	5	4	4	5	4
178	2	1	3	5	5	4
179	4	5	3	5	4	5
180	5	4	5	3	5	4
181	5	4	5	3	5	4
182	5	4	5	3	5	4
183	5	4	5	3	5	4
184	5	3	5	4	5	5
185	4	5	3	5	4	5
186	5	4	5	3	5	4
187	4	4	5	4	5	4
188	4	5	4	4	5	4
189	5	4	4	5	4	5
190	5	4	4	5	4	5
191	5	5	4	4	5	3
192	4	5	4	4	5	4
193	5	4	4	4	5	4
194	4	5	4	4	5	4
195	4	4	5	4	5	4
196	5	3	5	4	4	5
197	4	3	5	4	4	5
198	5	4	4	5	4	5
199	5	4	4	5	5	5
200	4	5	4	4	5	4
201	4	4	5	5	4	4
202	5	4	5	5	4	4
203	4	5	3	5	4	5
204	5	4	5	4	5	4

205	5	4	5	5	4	5
206	4	5	3	4	5	4
207	5	5	4	5	5	4
208	5	5	3	5	4	4
209	5	4	5	3	5	4
210	4	4	5	5	4	5
211	5	4	5	3	5	4
212	5	4	5	5	3	4
213	4	5	3	5	4	5
214	5	4	5	5	4	4
215	4	5	3	5	4	5
216	5	5	4	4	5	4
217	4	5	3	5	4	5
218	4	5	4	3	5	5
219	5	4	5	5	4	4
220	5	5	4	5	5	4
221	5	5	4	4	5	5
222	5	4	5	3	5	4
223	4	5	4	5	5	4
224	4	5	4	3	5	4
225	4	3	5	4	5	5
226	4	4	5	4	5	4
227	5	4	5	4	4	5
228	4	5	4	4	5	4
229	4	3	4	5	5	4
230	5	4	5	5	4	5
231	5	4	4	4	5	4
232	4	5	5	3	4	5
233	4	5	4	5	3	4
234	4	4	5	4	5	4
235	4	5	3	4	5	4
236	4	5	5	4	4	5
237	5	4	4	5	4	5
238	4	4	5	4	5	4
239	4	5	3	4	5	4
240	5	4	5	3	5	4
241	4	5	3	4	5	4
242	4	5	5	4	4	5

243	4	5	4	3	4	5
244	5	4	4	5	4	5
245	5	4	4	5	4	4
246	5	4	5	3	4	5
247	4	5	4	4	5	4
248	2	2	1	2	1	2
249	5	4	5	3	4	5
250	4	5	4	5	4	4
251	4	4	5	5	4	4
252	4	4	5	5	4	4
253	5	5	4	4	5	5
254	5	5	4	5	5	4
255	5	4	5	5	4	3
256	5	3	4	3	5	4
257	4	5	4	5	4	4
258	5	4	4	5	5	4
259	5	4	4	5	3	4
260	4	5	3	5	4	4
261	2	1	2	4	2	5
262	2	1	2	4	1	2
263	4	5	5	4	5	5
264	5	4	5	4	3	5
265	4	5	4	5	5	4
266	1	2	4	5	3	4
267	5	4	3	4	5	4
268	4	5	4	5	5	4
269	5	4	3	5	4	5
270	4	3	4	5	4	5
271	4	5	4	4	5	4
272	5	4	5	4	4	5
273	4	5	3	4	5	5
274	3	4	5	5	3	4
275	4	5	4	3	5	4
276	4	5	4	3	5	3
277	4	5	3	4	5	3
278	4	5	4	4	5	4
279	4	5	3	5	5	3
280	4	5	3	4	5	4

281	4	4	5	4	5	4
282	4	4	5	4	5	4
283	4	4	5	4	5	4
284	5	4	5	4	5	5
285	4	4	5	3	2	4
286	5	4	4	5	4	5
287	4	4	5	4	5	4
288	4	4	2	1	4	3
289	1	4	3	2	4	2
290	1	4	2	3	4	1
291	3	1	4	3	3	4
292	4	3	4	2	2	3
293	5	3	4	2	3	4
294	4	2	4	2	2	4
295	4	3	4	1	3	5
296	5	3	5	2	2	3
297	5	3	5	1	2	2
298	4	3	3	1	2	4
299	4	3	4	1	2	3
300	3	2	4	2	2	1
301	4	3	5	2	3	5
302	5	3	4	1	2	4
303	4	2	4	2	2	2
304	4	3	4	2	2	4
305	4	2	4	1	2	5
306	5	3	4	2	5	4
307	4	4	4	4	2	4
308	4	3	3	2	4	2
309	5	4	4	4	4	1
310	4	3	4	1	3	4
311	4	3	3	2	2	5
312	4	4	4	2	3	5
313	4	3	4	1	3	5
314	4	3	4	1	1	4
315	4	3	5	2	3	4
316	4	4	3	3	2	5
317	4	3	4	1	3	5
318	4	5	5	5	4	2

319	4	4	5	2	3	4
320	4	3	3	2	1	3
321	5	3	5	1	2	3
322	4	3	5	3	2	5
323	4	3	4	2	3	4
324	4	3	1	2	3	4
325	4	3	5	2	1	4
326	5	3	5	2	3	4
327	4	3	4	1	2	4
328	4	4	4	2	2	4
329	4	3	4	2	5	3
330	4	3	4	1	2	5
331	5	3	3	4	3	4
332	4	4	4	2	3	4
333	4	4	5	2	2	1
334	4	4	5	2	4	2
335	4	3	4	2	2	4
336	4	3	4	1	2	3
337	4	2	3	1	2	3
338	4	4	3	3	4	2
339	3	5	4	1	2	2
340	3	3	4	1	4	2
341	4	3	2	3	4	2
342	4	4	3	1	4	2
343	3	4	4	2	4	3
344	3	5	4	3	4	3
345	3	4	3	3	3	3
346	3	4	4	3	4	3
347	3	4	3	3	5	3
348	4	5	5	4	4	4
349	5	5	4	4	4	4
350	4	5	4	5	4	5
351	5	3	5	4	5	5
352	4	4	5	4	5	5
353	5	5	3	5	4	4
354	4	5	3	5	4	4
355	5	5	4	5	3	5
356	5	4	5	4	3	4

357	5	5	4	5	4	4
358	4	5	4	4	5	4
359	4	5	4	5	5	4
360	4	3	4	5	5	4
361	3	4	4	5	4	5
362	4	4	5	3	4	4
363	3	4	4	5	4	5
364	4	4	5	4	5	5
365	3	4	4	5	4	5
366	4	3	5	4	5	4
367	4	3	5	4	5	3
368	4	3	5	4	5	3
369	5	3	5	4	5	3
370	4	3	5	4	5	3
371	5	4	5	3	4	4
372	5	5	4	4	5	3
373	4	5	3	4	5	3
374	3	5	3	5	5	4
375	4	4	5	4	3	4
376	5	4	4	5	5	4
377	5	4	4	3	4	4
378	5	5	4	4	5	3
379	5	4	5	3	5	3
380	4	5	4	5	5	4
381	4	5	5	4	5	4
382	5	4	4	5	4	5
383	3	5	5	4	5	4
384	5	4	5	5	4	5

Lampiran 3 Hasil Uji Statistik

Hasil Output Validitas Literasi Digital (X1)

Correlations										
		X1. P1	X1. P2	X1. P3	X1. P4	X1. P5	X1. P6	X1. P7	X1. P8	Total X1
X1.P 1	Pearso n Correla tion	1	.041	.303 **	.134 **	.055	.268 **	.124 *	.228 **	.420* *
	Sig. (2- tailed)		.427	.000	.009	.281	.000	.015	.000	.000
	N	384	384	384	384	384	384	384	384	384
X1.P 2	Pearso n Correla tion	.041	1	.245 **	.502 **	.242 **	.237 **	.391 **	.233 **	.666* *
	Sig. (2- tailed)	.427		.000	.000	.000	.000	.000	.000	.000
	N	384	384	384	384	384	384	384	384	384
X1.P 3	Pearso n Correla tion	.303 **	.245 **	1	.133 **	.259 **	.269 **	.295 **	.374 **	.624* *
	Sig. (2- tailed)	.000	.000		.009	.000	.000	.000	.000	.000
	N	384	384	384	384	384	384	384	384	384
X1.P 4	Pearso n Correla tion	.134 **	.502 **	.133 **	1	.097 **	.259 **	.360 **	.211 **	.639* *
	Sig. (2- tailed)	.009	.000	.009		.058	.000	.000	.000	.000
	N	384	384	384	384	384	384	384	384	384
X1.P 5	Pearso n Correla tion	.055	.242 **	.259 **	.097	1	.006	.254 **	.178 **	.480* *
	Sig. (2- tailed)	.281	.000	.000	.058		.914	.000	.000	.000
	N	384	384	384	384	384	384	384	384	384
X1.P 6	Pearso n	.268 **	.237 **	.269 **	.259 **	.006	1	.097	.184 **	.480* *

	Correlation									
	Sig. (2-tailed)	.000	.000	.000	.000	.914		.057	.000	.000
	N	384	384	384	384	384	384	384	384	384
X1.P7	Pearson Correlation	.124*	.391**	.295**	.360**	.254**	.097	1	.158**	.629*
	Sig. (2-tailed)	.015	.000	.000	.000	.000	.057		.002	.000
	N	384	384	384	384	384	384	384	384	384
X1.P8	Pearson Correlation	.228**	.233**	.374**	.211**	.178**	.184**	.158**	1	.545*
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.002		.000
	N	384	384	384	384	384	384	384	384	384
Total X1	Pearson Correlation	.420**	.666**	.624**	.639**	.480**	.480**	.629**	.545**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	
	N	384	384	384	384	384	384	384	384	384
**. Correlation is significant at the 0.01 level (2-tailed).										
*. Correlation is significant at the 0.05 level (2-tailed).										

Hasil Output Validitas Keamanan Data Pribadi (X2)

Correlations		X2.P1	X2.P2	X2.P3	X2.P4	X2.P5	X2.P6	TotalX2
X2.P1	Pearson Correlation	1	-.034	.343**	.276**	.064	.260**	.487**
	Sig. (2-tailed)		.503	.000	.000	.208	.000	.000
	N	384	384	384	384	384	384	384
X2.P2	Pearson	-.034	1	.033	.453	.436	.191	.594**

	Correlation				**	**	**	
	Sig. (2-tailed)	.503		.519	.000	.000	.000	.000
	N	384	384	384	384	384	384	384
X2.P3	Pearson Correlation	.343**	.033	1	.181**	.212**	.259**	.535**
	Sig. (2-tailed)	.000	.519		.000	.000	.000	.000
	N	384	384	384	384	384	384	384
X2.P4	Pearson Correlation	.276**	.453**	.181**	1	.409**	.298**	.768**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000
	N	384	384	384	384	384	384	384
X2.P5	Pearson Correlation	.064	.436**	.212**	.409**	1	.114*	.654**
	Sig. (2-tailed)	.208	.000	.000	.000		.025	.000
	N	384	384	384	384	384	384	384
X2.P6	Pearson Correlation	.260**	.191**	.259**	.298**	.114*	1	.554**
	Sig. (2-tailed)	.000	.000	.000	.000	.025		.000
	N	384	384	384	384	384	384	384
TotalX2	Pearson Correlation	.487**	.594**	.535**	.768**	.654**	.554**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	
	N	384	384	384	384	384	384	384
**. Correlation is significant at the 0.01 level (2-tailed).								
*. Correlation is significant at the 0.05 level (2-tailed).								

Hasil Output Kewaspadaan Terhadap Penipuan Digital (Y)

Correlations								
		Y.P1	Y.P2	Y.P3	Y.P4	Y.P5	Y.P6	Total Y
Y.P1	Pearson Correlation	1	.142*	.335*	.154*	.180*	.298*	.527*
	Sig. (2-tailed)		.005	.000	.003	.000	.000	.000
	N	384	384	384	384	384	384	384
Y.P2	Pearson Correlation	.142*	1	.054	.386*	.488*	.188*	.627*
	Sig. (2-tailed)	.005		.289	.000	.000	.000	.000
	N	384	384	384	384	384	384	384
Y.P3	Pearson Correlation	.335*	.054	1	.057	.221*	.285*	.486*
	Sig. (2-tailed)	.000	.289		.265	.000	.000	.000
	N	384	384	384	384	384	384	384
Y.P4	Pearson Correlation	.154*	.386*	.057	1	.403*	.364*	.697*
	Sig. (2-tailed)	.003	.000	.265		.000	.000	.000
	N	384	384	384	384	384	384	384
Y.P5	Pearson Correlation	.180*	.488*	.221*	.403*	1	.182*	.697*
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000
	N	384	384	384	384	384	384	384
Y.P6	Pearson	.298*	.188*	.285*	.364*	.182*	1	.622*

	Correlation	*	*	*	*	*		*
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000
	N	384	384	384	384	384	384	384
Total Y	Pearson Correlation	.527*	.627*	.486*	.697*	.697*	.622*	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	
	N	384	384	384	384	384	384	384
**. Correlation is significant at the 0.01 level (2-tailed).								

Hasil uji Realibilitas Literasi Digital (X1)

Reliability Statistics	
Cronbach's Alpha	N of Items
.693	8

Hasil uji Realibilitas Keamanan Data Pribadi (X2)

Reliability Statistics	
Cronbach's Alpha	N of Items
.654	6

Hasil uji Realibilitas Kewaspadaan Terhadap Penipuan Digital (Y)

Reliability Statistics	
Cronbach's Alpha	N of Items
.668	6

Lampiran 4 Hasil Uji Asumsi Klasik

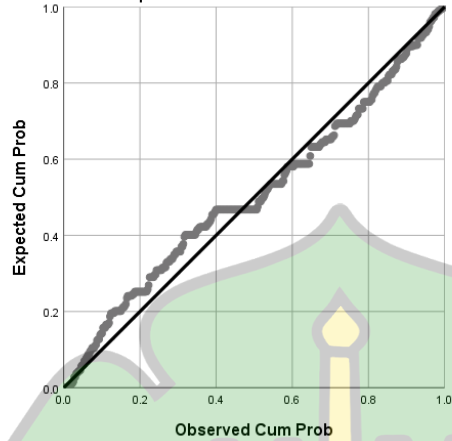
1. Hasil Uji Normalitas

One-Sample Kolmogorov-Smirnov Test			
			Unstandardized Residual
N			384
Normal Parameters ^{a,b}	Mean		.0000000
	Std. Deviation		1.69852692
Most Extreme Differences	Absolute		.083
	Positive		.062
	Negative		-.083
Test Statistic			.083
Asymp. Sig. (2-tailed)			.000 ^c
Monte Carlo Sig. (2-tailed)	Sig.		.008 ^d
	99% Confidence Interval	Lower Bound	.006
		Upper Bound	.010
a. Test distribution is Normal.			
b. Calculated from data.			
c. Lilliefors Significance Correction.			
d. Based on 10000 sampled tables with starting seed 2000000.			

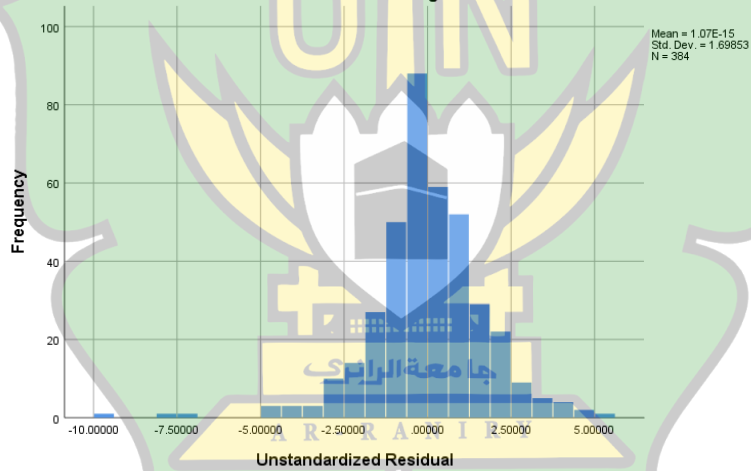
جامعة الرانري

A R - R A N I R Y

Normal P-P Plot of Regression Standardized Residual
Dependent Variable: TotalY



Histogram

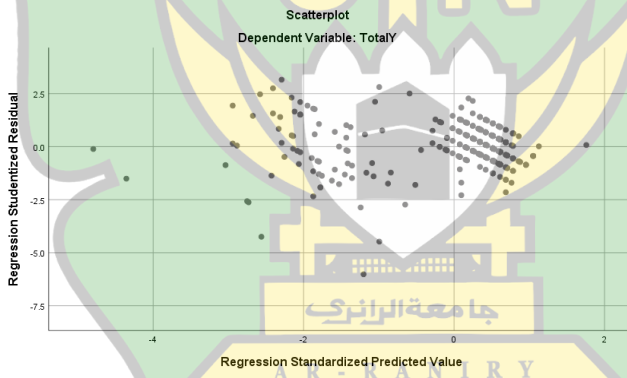


2. Hasil Uji Multikolinearitas

Coefficients ^a								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	.599	.701		.854	.393		
	TotalX1	.516	.040	.620	12.862	.000	.273	3.658
	TotalX2	.287	.050	.279	5.787	.000	.273	3.658

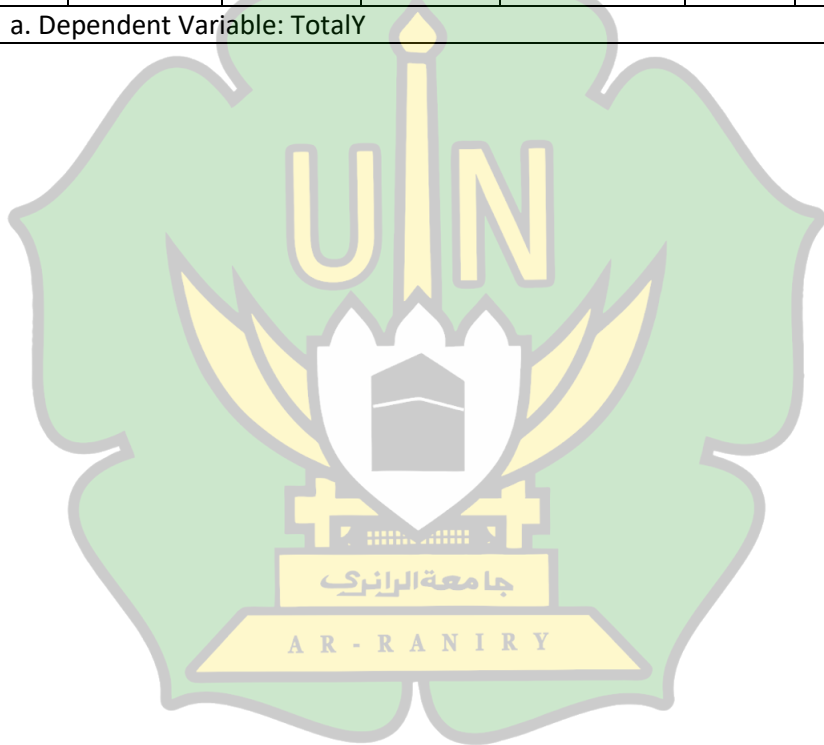
a. Dependent Variable: TotalY

3. Hasil Uji Heteroskedastisitas



Lampiran 5 Hasil Uji Regresi Linear Berganda

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.599	.701		.854	.393
	TotalX1	.516	.040	.620	12.862	.000
	TotalX2	.287	.050	.279	5.787	.000
a. Dependent Variable: TotalY						



Lampiran 6 Hasil Uji Hipotesis

1. Hasil Uji T (parsial)

Coefficients^a						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.599	.701		.854	.393
	TotalX1	.516	.040	.620	12.862	.000
	TotalX2	.287	.050	.279	5.787	.000
a. Dependent Variable: TotalY						

2. Hasil Uji F (simultan)

ANOVA^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3456.037	2	1728.018	595.840	.000 ^b
	Residual	1104.953	381	2.900		
	Total	4560.990	383			
a. Dependent Variable: TotalY						
b. Predictors: (Constant), TotalX2, TotalX1						

3. Hasil Uji Determinasi (R²)

Model Summary^b				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.870 ^a	.758	.756	1.703
a. Predictors: (Constant), TotalX2, TotalX1				
b. Dependent Variable: TotalY				

Lampiran 7 Tabel R

Tabel R Untuk 1-500					
By @SUJI DATA					
348	0.0881	0.1049	0.1243	0.1375	0.1752
349	0.0879	0.1047	0.1241	0.1373	0.1749
350	0.0878	0.1046	0.1240	0.1371	0.1747
351	0.0877	0.1044	0.1238	0.1369	0.1744
352	0.0876	0.1043	0.1236	0.1367	0.1742
353	0.0874	0.1041	0.1234	0.1366	0.1739
354	0.0873	0.1040	0.1233	0.1364	0.1737
355	0.0872	0.1038	0.1231	0.1362	0.1734
356	0.0871	0.1037	0.1229	0.1360	0.1732
357	0.0870	0.1035	0.1227	0.1358	0.1730
358	0.0868	0.1034	0.1226	0.1356	0.1727
359	0.0867	0.1032	0.1224	0.1354	0.1725
360	0.0866	0.1031	0.1222	0.1352	0.1722
361	0.0865	0.1030	0.1221	0.1350	0.1720
362	0.0863	0.1028	0.1219	0.1349	0.1718
363	0.0862	0.1027	0.1217	0.1347	0.1715
364	0.0861	0.1025	0.1216	0.1345	0.1713
365	0.0860	0.1024	0.1214	0.1343	0.1711
366	0.0859	0.1023	0.1212	0.1341	0.1708
367	0.0858	0.1021	0.1211	0.1339	0.1706
368	0.0856	0.1020	0.1209	0.1338	0.1704
369	0.0855	0.1018	0.1207	0.1336	0.1702
370	0.0854	0.1017	0.1206	0.1334	0.1699
371	0.0853	0.1016	0.1204	0.1332	0.1697
372	0.0852	0.1014	0.1203	0.1330	0.1695
373	0.0851	0.1013	0.1201	0.1329	0.1693
374	0.0850	0.1012	0.1199	0.1327	0.1690
375	0.0848	0.1010	0.1198	0.1325	0.1688
376	0.0847	0.1009	0.1196	0.1323	0.1686
377	0.0846	0.1008	0.1195	0.1322	0.1684
378	0.0845	0.1006	0.1193	0.1320	0.1682
379	0.0844	0.1005	0.1191	0.1318	0.1679
380	0.0843	0.1004	0.1190	0.1316	0.1677
381	0.0842	0.1002	0.1188	0.1315	0.1675
382	0.0841	0.1001	0.1187	0.1313	0.1673
383	0.0840	0.1000	0.1185	0.1311	0.1671
384	0.0838	0.0998	0.1184	0.1310	0.1668
385	0.0837	0.0997	0.1182	0.1308	0.1666
386	0.0836	0.0996	0.1181	0.1306	0.1664