

**PENGARUH ANCAMAN *PHISING* DAN PRINSIP KEHATI-
HATIAN TERHADAP TINGKAT KEPERCAYAAN NASABAH
PENGUNA *MOBILE BANKING***

Skripsi

*Diajukan untuk Memenuhi Salah Satu Syarat guna Memperoleh
Gelar Sarjana Ekonomi (S.E) pada Program Studi Perbankan Syariah
Fakultas Ekonomi dan Binsis Islam Universitas Islam Negeri Palopo*



Diajukan Oleh:

MUH. FIKRI HAIKAL

20 0402 0096

**PROGRAM STUDI PERBANKAN SYARIAH
FAKULTAS EKONOMI DAN BISNIS ISLAM
UNIVERSITAS ISLAM NEGERI PALOPO
2025**

**PENGARUH ANCAMAN *PHISING* DAN PRINSIP KEHATI-
HATIAN TERHADAP TINGKAT KEPERCAYAAN NASABAH
PENGUNA *MOBILE BANKING***

Skripsi

*Diajukan untuk Memenuhi Salah Satu Syarat guna Memperoleh
Gelar Sarjana Ekonomi (S.E) pada Program Studi Perbankan Syariah
Fakultas Ekonomi dan Binsis Islam Universitas Islam Negeri Palopo*



Diajukan Oleh:

MUH. FIKRI HAIKAL

20 0402 0096

Pembimbing:

Muh. Ginanjar, S.E., M.M.

**PROGRAM STUDI PERBANKAN SYARIAH
FAKULTAS EKONOMI DAN BISNIS ISLAM
UNIVERSITAS ISLAM NEGERI PALOPO
2025**

HALAMAN PERNYATAAN KEASLIAN

Saya yang bertandatangan di bawah ini:

Nama : Muh. Fikri Haikal
Nim : 2004020096
Fakultas : Ekonomi dan Bisnis Islam
Program Studi : Perbankan Syariah

Menyatakan dengan sebenarnya bahwa:

1. Skripsi ini merupakan hasil karya saya sendiri, bukan plagiasi atau duplikasi dari tulisan/karya orang lain yang saya akui sebagai tulisan atau pikiran saya sendiri,
2. Seluruh bagian dari skripsi ini adalah karya saya sendiri selain kutipan yang ditunjukkan sumbernya. Segala kekeliruan dan atau kesalahan yang ada di dalamnya adalah tanggungjawab saya.

Bila mana di kemudian hari pernyataan ini tidak benar, maka saya bersedia menerima sanksi administrative atas perbuatan tersebut dan gelar akademik yang saya peroleh karenanya dibatalkan.

Demikian pernyataan ini dibuat untuk dipergunakan sebagai mana mestinya.

Palopo, 6 April 2026

Buat pernyataan,



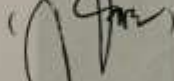
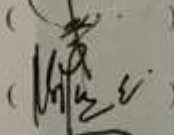
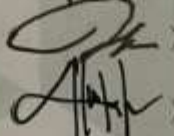

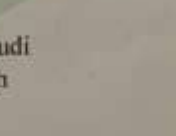
Muh. Fikri Haikal
NIM 2004020096

HALAMAN PENGESAHAN

Skripsi berjudul Pengaruh Ancaman *Phising* dan Prinsip Kehati-Hatian terhadap Tingkat Kepercayaan Nasabah Pengguna *Mobile Banking* yang ditulis oleh Muh. Fikri Haikal Nomor Induk Mahasiswa (NIM) 2004020096, mahasiswa Program Studi Perbankan Syariah dan Bisnis Islam Universitas Islam Negeri Palopo, yang dimunaqasyahkan pada hari Rabu, tanggal 21 Januari 2026 Miladiyah bertepatan dengan 2 Sya'ban 1447 Hijriah telah diperbaiki sesuai catatan dan permintaan Tim Penguji, dan diterima sebagai syarat meraih gelar Sarjana Ekonomi (S.E).

Palopo, 01 April 2026

TIM PENGUJI

- | | | |
|--|-------------------|---|
| 1. Dr. Hj. Anita Marwing, S.H.I, M.H. I. | Ketua Sidang | () |
| 2. Ilham, S.Ag., M.A. | Sekretaris Sidang | () |
| 3. Dr. Hj. Salmilah, S.Kom., M.T. | Penguji I | () |
| 4. Dr. Adzan Noor Bakri, S.E.Sy., MA.Ek. | Penguji II | () |
| 5. Muh. Ginanjar, S.E., M.M. | Pembimbing | () |

Mengetahui:

a.n. Rektor UIN Palopo
Dekan Fakultas Ekonomi dan Bisnis Islam



Dr. Hj. Anita Marwing, S.H.I., M.H.I.
NIP. 198201242009012006

Ketua Program Studi
Perbankan Syariah



Edi Indra Setiawan, S.E., M.M.
NIP. 198912072019031005

PRAKATA

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ
الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ وَالصَّلَاةُ وَالسَّلَامُ مَعْلَمًا شَرَفًا لَأَنْبِيَاءِ وَالْمُرْسَلِينَ سَيِّدِنَا مُحَمَّدٍ وَعَالِهِ وَاصْحَابِهِ
(هـ) (اما بعد)

Alhamdulillah, segala puji dan syukur penulis panjatkan kepada Allah *Subhanahu Wata'ala* yang telah menganugerahkan rahmat, hidayah serta kekuatan lahir dan batin. Salawat dan salam kepada Nabi Muhammad saw., kepada para keluarga, sahabat dan pengikut-pengikutnya. Sehingga penulis dapat menyelesaikan penulisan skripsi ini dengan judul “Pengaruh Ancaman *Phising* dan Prinsip Kehati-Hatian terhadap Tingkat Kepercayaan Nasabah Pengguna *Mobile Banking*” tepat waktu dan dengan hasil yang sesuai dengan harapan.

Penulis menyadari bahwa dalam penyelesaian skripsi ini, penulis menghadapi banyak rintangan dan kesulitan. Namun, dengan pertolongan Allah *Subhanahu Wata'ala*, ketekunan dan ketabahan penulis yang disertai dengan dukungan dan doa dari berbagai pihak sehingga Alhamdulillah skripsi ini dapat terselesaikan dengan baik.

Terkhusus kepada kedua orang tuaku tercinta ayahanda dan ibunda, yang telah mengasuh dan mendidik penulis dengan penuh kasih sayang sejak kecil hingga sekarang dan segala yang telah diberikan kepada anak-anaknya serta saudariku yang selama ini membantu mendoakanku. Semoga Allah SWT., mengumpulkan kita semua dalam surga-Nya kelak.

Selanjutnya penulis juga mengucapkan terimah kasih kepada semua pihak yaitu:

1. Dr. Abbas Langaji, M.Ag. selaku Rektor UIN Palopo, beserta Dr.Murni Yusuf, M.Pd. selaku Wakil Rektor Bidang Akademik, dan Pengembangan Kelembagaan, Dr. Masruddin, S.S., M.Hum. selaku Wakil Rektor Bidang Administrasi Umum, Perencanaan, dan Keuangan, dan Dr. Mustaming, S.Ag., M.HI selaku Wakil Rektor Bidang Kemahasiswaan dan Kerja Sama yang telah membina dan berupaya meningkatkan mutu perguruan tinggi ini.
2. Dr. Hj. Anita Marwing, S.HI., M.HI, selaku Dekan Fakultas Ekonomi dan Bisnis Islam UIN Palopo, beserta Wakil Dekan Bidang Akademik, Ilham, S.Ag., M.A., Wakil Dekan Bidang Administrasi Umum, Perencanaan, dan Keuangan, Dr. Alia Lestari, M.Si dan Wakil Dekan Bidang Kemahasiswaan dan Kerja Sama, Muhammad Ilyas. S.Ag., M.A yang telah banyak memberikan petunjuk sehingga skripsi ini dapat terselesaikan
3. Edi Indra Setiawan S.E., M.M, selaku Ketua Program Studi Perbankan Syari'ah di UIN Palopo beserta staf yang telah membantu dan mengarahkan dalam penyelesaian skripsi.
4. Muh Ginanjar, S.E., M.M. selaku pembimbing yang telah membantu saya dalam penyelesaian skripsi ini dan seluruh dosen beserta staf pegawai UIN Palopo yang telah mendidik penulis selama berada di UIN Palopo dan memberikan bantuan dalam penyusunan skripsi ini.
5. Abubakar, S.Pd.I, M.Pd. selaku Pimpinan Perpustakaan beserta karyawan dan karyawati dalam ruang lingkup UIN Palopo, yang telah banyak membantu, khususnya dalam mengumpulkan literatur yang berkaitan dengan pembahasan skripsi ini.
6. Kepada semua teman-teman seperjuangan terkhusus Perbankan Syariah angkatan 2020, yang telah banyak membantu selama penulis menuntut ilmu di UIN Palopo mulai tahun 2020 sampai sekarang.
7. Kepada seluruh keluarga besar peneliti, baik dari pihak Bapak ataupun Ibu, peneliti mengucapkan terimakasih banyak atas semua semangat yang sudah

diberikan, serta dukungan secara mental yang akan selalu peneliti ingat.

8. Kepada yang terspesial: Nur Afina Inaya, S.Pd yang selalu membantu dan mensupport penulis dalam setiap langka untuk menyelesaikan pendidikan di UIN Palopo.
9. Kepada seluruh sahabat refleksi saya di UKK Seni Sibola, Ayu Lestari, Khusnul Hatimah, Eny Erwanti, Cahyani Yasman, Amaliah Reskyta Baso, dan Akmal terima kasih banyak sudah memberikan motivasi dan saran sepanjang peneliti melewati masa perkuliahan hingga penyelesaian skripsi ini.

Semoga setiap bantuan Do'a, dukungan, motivasi, dorongan, kerjasama dan amal bakti yang telah diberikan kepada penulis mendapat balasan yang layak disisi Allah swt. Akhirnya penulis berharap semoga skripsi ini bermanfaat bagi setiap yang memerlukan dan semoga Allah swt. Menuntun kearah yang benar dan lurus. Aamiin.

Palopo, 20 Mei 2025

Muh Fikri Haikal
NIM:20 0402 0096

PEDOMAN TRANSLITERASI DAN SINGKATAN

Transliterasi adalah mengalihkan suatu tulisan ke dalam aksara misalnya, dari aksara Arab ke Aksara Latin. Berikut ini adalah surat keputusan Bersama Menteri Agama dan Menteri Pendidikan dan Kebudayaan RI Nomor: 158 Tahun 1987 – Nomor: 0543 b/u/1997 tentang Transliterasi Arab-Latin yang peneliti gunakan dalam penelitian skripsi ini.

1. Konsonan

Huruf Arab	Nama	Huruf Latin	Nama
ا	Alif	Tidak dilambangkan	Tidak dilambangkan
ب	Ba'	B	Te
ت	Ta'	T	Te
ث	Ša'	Š	es (dengan titik di atas)
ج	Jim.	J	Je
ح	Ha'	H	ha (dengan titik di bawah)
خ	Kha.	Kh	ka dan ha
د	Dal	D	De
ذ	Žal.	Ž.	zet (dengan titik di atas)
ر	Ra'	R	Er
ز	Zai	Z	Zet
س	Sin	S.	Es
ش	Syin	Sy	es dan ye
ص	Sad	S	es (dengan titik di bawah)
ض	Dad	D.	de (dengan titik

			bawah)
ط	Ta	T	te (dengan titik bawah).
ظ	Za	Z	zet (dengan titik bawah).
ع	‘ain	‘	apstrof terbalik
غ	Gain	G	Ge
ف	Fa	F	Ef
ق	Qaf	Q	Qi
ك	Kaf.	K	Ka
ل	Lam	L	El
م	Mim	M	Em
ن	Nun	N	En
و	Wau	W	We
ه	Ha	H	Ha
ء	Hamzah	,	Apostrof
ي	Ya	Y	Ye

Daftar huruf bahasa arab dan transliterasinya ke dalam huruf latin dapat dilihat dibawah ini:

Hamzah (ء) yang terletak di awal kata mengikuti vokalnya tanpa diberi tanda apa pun. Jika ia terletak di tengah atau di akhir, maka ditulis dengan tanda (’).

2. Vokal

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

Tanda Vokal	Nama	Latin	Keterangan
اَ	<i>Fathah</i>	A	Á
اِ	<i>Kasrah</i>	I	Í
اُ	<i>Dammah</i>	U	Ú

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

Tanda	Nama	Huruf Latin	Nama
اِي	<i>Fathah danyā'</i>	Ai	a dan i
اُو	<i>Fathah dan wau</i>	Au	a dan u

Contoh:

كَيْفَ : *kaifa*

هَوْلًا : *hauła*

3. Maddah

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

Harakat dan Huruf	Nama	Huruf dan Tanda	Nama
اِيَّ اِيَّ	<i>fathah dan alif</i> atau <i>yā</i>	Ā	a dan garis di atas

كَيْ	<i>kasrah dan yā'</i>	Ī	i dan garis di atas
و	<i>ḍammah dan wau</i>	Ū	u dan garis di atas

مَاتَ : māta

رَمَى : rāmā

قِيلَ : qīla

يَمُوتُ : yamūtu

4. *Tā marbūtah*

Transliterasi untuk *tā' marbūtah* ada dua, yaitu *tā' marbūtah* yang hidup atau mendapat harakat *fathah*, *kasrah*, dan *dammah*, transliterasinya adalah [t]. sedang *tā' marbūtah* yang mati atau mendapat harakat sukun, transliterasinya adalah [h].

Kalau pada kata yang berakhir dengan *tā' marbūtah* diikuti oleh kata yang menggunakan kata sandang *al-* serta bacaan kedua kata itu terpisah, maka *tā' marbūtah* itu ditransliterasikan dengan ha [h].

Contoh:

رَوْضَةَ الْأَطْفَالِ : *raudah al-atfāl*

الْمَدِينَةَ الْفَاضِلَةَ : *al-madīnah al-fādilah*

الْحِكْمَةَ : *al-hikmah*

5. Syaddah (*Tasydīd*)

Syaddah atau *tasydīd* yang dalam sistem tulisan Arab dilambangkan dengan sebuah tanda *tasydīd* (ّ), dalam transliterasi ini dilambangkan dengan perulangan huruf (konsonan ganda) yang diberi tanda *syaddah*.

Contoh:

رَبَّنَا : *rabbānā*

نَجَّيْنَا : *najjainā*

الْحَقَّ : *al-haqq*

نُعَمُّ : *nu'ima*

عَدُوُّ : *'aduwwun*

Jika huruf **ي** ber-*tasydid* di akhir sebuah kata dan didahului oleh huruf *kasrah* (**ـِ**), maka ia ditransliterasi seperti huruf *maddah* menjadi **ī**.

Contoh:

عَلِيٌّ : 'Alī (bukan 'Aliyy atau A'ly)

عَرَبِيٌّ : 'Arabī (bukan A'rabiyy atau 'Arabiy)

6. Kata Sandang

Kata sandang dalam sistem tulisan Arab dilambangkan dengan huruf **ال** (*alif lam ma'rifah*). Dalam pedoman transliterasi ini, kata sandang ditransliterasi seperti biasa , al-, baik ketika ia diikuti oleh huruf *syamsi yah* maupun huruf *qamariyah*. Kata sandang tidak mengikuti bunyi huruf langsung yang mengikutinya. Kata sandang ditulis terpisah dari kata yang mengikutinya dan dihubungkan dengan garis mendatar (-).

Contoh:

الشَّمْسُ : *al-syamsu* (bukan *asy-syamsu*)

الزَّلْزَلَةُ : *al-zalزالah* (bukan *az-zalزالah*)

الْفَلْسَفَةُ : *al-falsafah*

الْبِلَادُ : *al-bilādu*

7. Hamzah

Aturan transliterasi huruf hamzah menjadi apostrof (') hanya berlaku bagi hamzah yang terletak di tengah dan akhir kata. Namun, bila hamzah terletak di awal kata, ia tidak dilambangkan, karena dalam tulisan Arab ia berupa alif.

Contoh:

تَأْمُرُونَ : *ta'murūna*

النَّوْعُ : *al-nau'*

شَيْءٌ : *syai'un*

أُمِرْتُ : *umirtu*

8. Penulisan Kata Arab yang Lazim Digunakan dalam Bahasa Indonesia

Kata, istilah atau kalimat Arab yang ditransliterasi adalah kata, istilah atau kalimat yang belum dibakukan dalam bahasa Indonesia. Kata, istilah atau kalimat yang sudah lazim dan menjadi bagian dari perbendaharaan bahasa Indonesia, atau sering ditulis dalam tulisan bahasa Indonesia, atau lazim digunakan dalam dunia akademik tertentu, tidak lagi ditulis menurut cara transliterasi di atas. Misalnya, kata Al-Qur'an (dari *al-Qur'ān*), alhamdulillah, dan munaqasyah. Namun, bila kata-kata tersebut menjadi bagian dari satu rangkaian teks Arab, maka harus ditransliterasi secara utuh.

Contoh:

Syarh al-Arba'īn al-Nawāwī

Risālah fī Ri'āyah al-Maslahah

9. *Lafz al-Jalālah*

Kata “Allah swt.” yang didahului partikel seperti huruf jarr dan huruf lainnya atau berkedudukan sebagai *mudāfilaih* (frasa nominal), ditransliterasi tanpa huruf hamzah. Contoh:

بِاللَّهِ : *billāh*

دِينُ اللَّهِ : *dīnullāh*

Adapun *tā'marbūtah* di akhir kata yang disandarkan kepada *lafz al-jalālah*, diteransliterasi dengan huruf [t]. Contoh:

هُم فِي رَحْمَةِ اللَّهِ *hum fī rahmatillāh*

10. Huruf Kapital

Walau sistem tulisan Arab tidak mengenal huruf kapital (*All Caps*), dalam transliterasinya huruf-huruf tersebut dikenai ketentuan tentang penggunaan huruf kapital berdasarkan pedoman ejaan Bahasa Indonesia yang berlaku (EYD). Huruf kapital, misalnya, digunakan untuk menuliskan huruf awal nama diri (orang, tempat, bulan) dan huruf pertama pada permulaan kalimat. Bila nama diri didahului oleh kata sandang (al-), maka yang ditulis dengan huruf kapital tetap huruf awal nama diri tersebut, bukan huruf awal kata sandangnya. Jika terletak pada awal kalimat, maka huruf A dari kata sandang tersebut menggunakan huruf kapital (al-). Ketentuan yang sama juga berlaku untuk huruf awal dari judul referensi yang didahului oleh kata sandang al-, baik ketika ia ditulis dalam teks maupun dalam catatan rujukan (CK, DP, CDK, dan DR).

Contoh:

*Wa mā Muhammadun illā rasūl Inna awwala baitin wudi'a linnāsi lallazī bi
Bakkata mubārakan*

Syahru Ramadān al-lazī unzila fīhi al-Qurān

Nasīr al-Dīn al-Tūsī

Nasr Hāmid Abū Zayd

Al-Tūfī

Al-Maslahah fī al-Tasyrī' al-Islāmī

Jika nama resmi seseorang menggunakan kata Ibnu (anak dari) dan Abū (bapak dari) sebagai nama kedua terakhirnya, maka kedua nama terakhir itu harus disebutkan sebagai nama akhir dalam daftar pustaka atau daftar referensi.

Contoh:

Abū al-Walīd Muhammad ibn Rusyd, ditulis menjadi: Ibnu Rusyd, Abū al-Walīd Muhammad (bukan: Rusyd, Abū al-Walīd Muhammad Ibnu)
Nasr Hāmid Abū Zaīd, ditulis menjadi: Abū Zaīd, Nasr Hāmid (bukan, Zaīd, Nasr Hāmid Abū)

11. Singkatan

Swt.	: <i>Subhanahu wa ta 'ala</i>
Saw.	: <i>SallAllah swt.u 'alaihi wa sallam</i>
as	: <i>'alaihi al-salam</i>
ra	: <i>RadiAllah swt.u 'anha</i>
H	: Hijriyah
M	: Masehi
No.	: Nomor
Vol	: Volume
QS.	: Qur'an Surah
HR	: Hadist Riwayat

DAFTAR ISI

SAMPUL	
PRAKATA	i
PEDOMAN TRANSLITERASI DAN SINGKATAN	iv
DAFTAR ISI.....	xii
DAFTAR AYAT.....	xiii
DAFTAR TABEL	xiv
DAFTAR GAMBAR.....	xv
DAFTAR LAMPIRAN	xvi
ABSTRAK	xvii
ABSTRACT	xviii
BAB I PENDAHULUAN.....	1
A. Latar Belakang.....	1
B. Rumusan Masalah.....	10
C. Tujuan Penelitian.....	11
D. Manfaat Penelitian	11
BAB II KAJIAN TEORI	13
A. Penelitian Terdahulu yang Relevan.....	13
B. Landasan Teori	18
C. Kerangka Pikir.....	43
D. Hipotesis Penelitian	45
BAB III METODE PENELITIAN	46
A. Jenis Penelitian	46
B. Lokasi dan Waktu Penelitian	47
C. Defenisi Oprasional Variabel	47
D. Populasi dan Sampel.....	48
E. Teknik Pengumpulan	51
F. Instrumen Penelitian	52
G. Uji Validitas dan Reliabilitas.....	53
H. Teknik Analisis Data	54
BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....	58
A. Hasil Penelitian.....	58
B. Pembahasan	76
BAB V PENUTUP.....	81
A. Simpulan.....	81
B. Saran	82
DAFTAR PUSTAKA	
LAMPIRAN	

DAFTAR AYAT

Q.S. Al - Baqarah Ayat 188	19
Q.S. Al- Hujarat Ayat 6.....	31
Q.S. An - Nisa Ayat 29	35
Q.S. Al - Baqarah Ayat 282	37

DAFTAR TABEL

Tabel 3.1 Defenisi Operasional.....	48
Tabel 4.1 Jenis Kelamin Responden	64
Tabel 4.2 Usia Responden	65
Tabel 4.3 Hasil Uji Validitas.....	66
Tabel 4.4 Hasil Uji Reliabilitas	67
Tabel 4.5 Hasil Uji Normalitas	68
Tabel 4.6 Hasil Uji Multikolinearitas	69
Tabel 4.7 Hasil Uji Heterokedastisitas	70
Tabel 4.8 Hasil Uji Regresi Linear Berganda	71
Tabel 4.9 Hasil Uji T.....	72
Tabel 4.10 Hasil Uji F.....	74
Tabel 4.11 Hasil Uji Koefisien Determinasi	75

DAFTAR GAMBAR

Gambar 2.1 Kerangka Pikir	43
Gambar 4.1 Logo Bank Syariah Indonesia (BSI)	58
Gambar 4.2 Struktur Organisasi BSI KCP Palopo.....	61

DAFTAR LAMPIRAN

Lampiran 1 Kuesioner

Lampiran 2 Hasil Kuesioner

Lampiran 3 Hasil Olah Data Kuesioner

Lampiran 4 F Tabel

Lampiran 5 T tabel

Lampiran 6 R Tabel

ABSTRAK

Muh Fikri Haikal, 2025 “Pengaruh Ancaman *Phishing* dan Prinsip Kehati-Hatian Terhadap Tingkat Kepercayaan Nasabah Pengguna *Mobile Banking*”. Skripsi Program Studi Perbankan Syariah Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Palopo. Dibimbing oleh Muh Ginanjar, S.E., M.M.

Penelitian ini membahas pengaruh ancaman *phishing* dan prinsip kehati-hatian terhadap tingkat kepercayaan nasabah pengguna *mobile banking*. Latar belakang penelitian ini didasari oleh pesatnya perkembangan layanan perbankan digital yang diiringi dengan meningkatnya risiko kejahatan siber, khususnya *phishing*, yang dapat mengancam keamanan data serta menurunkan kepercayaan nasabah. Di sisi lain, penerapan prinsip kehati-hatian menjadi faktor penting dalam meminimalisir risiko tersebut dan menjaga kepercayaan nasabah dalam menggunakan layanan *mobile banking*. Tujuan penelitian ini adalah untuk mengetahui pengaruh ancaman *phishing* dan prinsip kehati-hatian secara parsial maupun simultan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*.

Metode penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian asosiatif (kausal). Populasi penelitian adalah mahasiswa Fakultas Ekonomi dan Bisnis Islam UIN Palopo sebanyak 2.575 orang. Teknik pengambilan sampel menggunakan *non-probability sampling* dengan metode *purposive sampling*, dengan kriteria mahasiswa yang memiliki rekening dan menggunakan *mobile banking* pada periode Januari 2024 hingga Juni 2025. Jumlah sampel sebanyak 100 responden. Pengumpulan data dilakukan melalui kuesioner *skala Likert* dan dianalisis menggunakan regresi linier berganda dengan bantuan SPSS versi 26.

Hasil penelitian menunjukkan bahwa secara parsial ancaman *phishing* dan prinsip kehati-hatian berpengaruh signifikan terhadap tingkat kepercayaan nasabah. Secara simultan, kedua variabel tersebut juga berpengaruh signifikan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*. Dengan demikian, peningkatan prinsip kehati-hatian dan pengendalian terhadap ancaman *phishing* dapat meningkatkan kepercayaan nasabah.

Kata Kunci: Ancaman *Phishing*, Kepercayaan Nasabah, *Mobile Banking*, Prinsip Kehati-hatian

ABSTRACT

Muh Fikri Haikal, 2025. *“The Influence of Phishing Threats and the Precautionary Principle on the Level of Customer Trust of Mobile Banking Users”*. Thesis of the Islamic Banking Study Program, Faculty of Islamic Economics and Business, State Islamic Institute of Palopo. Supervised by Muh Ginanjar, S.E., M.M.

This study discusses the influence of phishing threats and the principle of prudence on the level of customer trust of mobile banking users. The background of this research is based on the rapid development of digital banking services accompanied by the increasing risk of cybercrime, especially phishing, which can threaten data security and reduce customer trust. On the other hand, the application of the principle of prudence is an important factor in minimizing these risks and maintaining customer confidence in using mobile banking services. The purpose of this study is to determine the influence of phishing threats and the principle of prudence partially or simultaneously on the level of customer trust of mobile banking users.

This research method uses a quantitative approach with the type of associative (causal) research. The research population is 2,575 students of the Faculty of Islamic Economics and Business UIN Palopo. The sampling technique uses non-probability sampling with the purposive sampling method, with the criteria of students who have an account and use mobile banking in the period from January 2024 to June 2025. The sample size was 100 respondents. Data collection was carried out through a Likert scale questionnaire and analyzed using multiple linear regression with the help of SPSS version 26.

The results of the study show that partially the threat of phishing and the precautionary principle have a significant effect on the level of customer trust. Simultaneously, these two variables also have a significant effect on the level of customer confidence of mobile banking users. Thus, increasing the principle of prudence and control against phishing threats can increase customer trust.

Keywords: *Phishing Threats, Customer Trust, Mobile Banking, Caution Principles*

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan teknologi yang sangat pesat membuat meningkatnya pula masyarakat yang menggunakan layanan internet. Beberapa pihak berbondong-bondong membuat suatu pembaruan yang dapat diminati di kalangan masyarakat. Salah satu pembaruan ialah dalam bidang perbankan. Ketika dahulu masyarakat yang ingin mengambil uang, mentransfer uang, dan melakukan transaksi lainnya dapat pergi ke salah satu bank yang terdekat dan biasanya diharuskan untuk mengantri. Akan tetapi sekarang masyarakat dipermudah dengan diciptakannya suatu inovasi dibidang perbankan berupa *electronic banking (e-banking)* yang berbasis internet.

Pengembangan perbankan digital berbasis layanan elektronik bertujuan untuk memaksimalkan informasi nasabah agar dapat memberikan pelayanan yang lebih nyaman dan sesuai dengan kebutuhan mereka. Teknologi aplikasi perbankan berbasis fitur *mobile*, yang disebut dengan *digital banking*, mencakup layanan seperti *SMS banking*, *phone banking*, *Mobile Banking*, serta ATM. Beberapa bank bahkan telah meluncurkan layanan perbankan tanpa cabang, yang dirancang khusus untuk Masyarakat yang belum memiliki akses ke layanan perbankan. Ini berarti bahwa layanan yang diberikan oleh *customer service* dan *back office* harus berjalan dengan cepat, serta system pengumpulan pembayaran harus dilakukan secara

digital.¹

Tersedianya fasilitas yang ditawarkan oleh masing-masing bank untuk mempermudah aktifitas sehari-hari melalui *Mobile Banking* diantaranya, pengecekan saldo rekening, transfer dana antar rekening maupun bank, pemesanan tiket, pembayaran tagihan listrik, air, telepon maupun internet yang mendorong ketertarikan masyarakat untuk menggunakan *Mobile banking*. Dengan demikian sektor perbankan harus meningkatkan kinerja serta fasilitas-fasilitas dalam mendukung penggunaan *Mobile Banking* dengan merujuk sesuai ketentuan yang telah diatur dalam Undang-Undang No. 7 Tahun 1992 yang diubah menjadi UU No. 10 Tahun 1998 tentang Perbankan.²

Dalam *website* Bank Syariah Indonesia dijelaskan bahwa sampai dengan semester I/2024, nilai transaksi melalui BSI *Mobile* telah mencapai Rp298,82 triliun, tumbuh 35,4% secara tahunan atau *year on year* (yoy). Jumlah pengguna BSI *Mobile* juga ikut melonjak dari Desember 2023 mencapai 12,72% (YtD) per Juni 2024 menjadi 7,12 juta orang. Pada periode tersebut, BSI *mobile* mencatatkan jumlah transaksi sebanyak 247,32 juta.

Salah satu bentuk perwujudan terhadap pesatnya perkembangan bank Syariah yaitu dengan adanya penggabungan (merger) 3 bank Syariah yaitu Bank Syariah Mandiri (BSM), Bank BNI Syariah dan Bank BRI Syariah menjadi Bank Syariah Mandiri (BSI). Penggabungan dari ketiga bank tersebut dilakukan sebagai

¹ Priska Cintya Amarta, "Pengaruh Teknologi Digital Dalam Perkembangan Layanan Perbankan Syariah," *Jurnal Ilmiah Research and Development Student (JIS)* 2, no. 3 (2024): 134–45, <https://doi.org/https://doi.org/10.59024/jise.v2i3.788>.

² Dewan Perwakilan Rakyat Republik Indonesia, "Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan" (Indonesia, N.D.).

upaya untuk menjadi pilar baru kekuatan ekonomi nasional dan mendorong Indonesia sebagai pusat ekonomi dan keuangan Syariah global³.

Namun di era digital seperti sekarang ini industri keuangan syariah, termasuk BSI, menghadapi risiko keamanan yang semakin kompleks. Salah satu risiko terbesar adalah peretasan, yang dapat menyebabkan terungkapnya informasi nasabah dan merusak kepercayaan publik terhadap bank. Baru-baru ini, BSI menghadapi tantangan signifikan terkait insiden teknis dan keamanan. Salah satu insiden yang paling menonjol adalah insiden BSI Error yang terjadi pada akhir bulan Mei 2023 dan mempengaruhi operasional bank sehari-hari. Selain itu, dugaan peretasan juga muncul, sehingga meningkatkan kekhawatiran tentang keamanan data dan informasi pelanggan. Menurut laporan yang beredar di media massa, insiden tersebut membuat nasabah merasa khawatir dan tidak percaya terhadap keamanan data mereka di bank tersebut. Selain itu, insiden tersebut juga membuat nasabah merasa tidak nyaman dan kesulitan dalam melakukan transaksi. Kejadian ini menimbulkan pertanyaan serius mengenai kesiapan teknis dan keamanan BSI dalam menghadapi tantangan modern dan dampaknya terhadap kepercayaan nasabah.⁴

Kepercayaan dan loyalitas nasabah merupakan faktor kunci di sektor perbankan, termasuk di sektor perbankan syariah. Kepercayaan nasabah terhadap lembaga keuangan syariah mencerminkan keyakinan mereka terhadap kejujuran,

³ Bank Syariah Indonesia, "Digital Banking Dinilai Optimal, BSI Raih Penghargaan Best Digital Bank," <https://www.bankbsi.co.id/>, accessed September 17, 2024, <https://www.bankbsi.co.id/news-update/berita/digital-banking-dinilai-optimal-bsi-raih-penghargaan-best-digital-bank>.

⁴ Lutfi Maulana and Nadia Nur Fitriana, "Analisis Dampak Insiden BSI Error Dan Dugaan Hacking Bank Syariah Indonesia (BSI) Terhadap Kepercayaan Dan Loyalitas Nasabah Bank Syariah Indonesia Di Kabupaten Subang," *Rayah Al-Islam*, 2024.

transparansi dan kepatuhan terhadap prinsip syariah dalam berbisnis.⁵ Kepercayaan ini memberikan dasar yang kuat untuk membangun hubungan jangka panjang antara nasabah dan Lembaga keuangan syariah, yang pada gilirannya memberikan kontribusi terhadap stabilitas dan pertumbuhan seluruh sektor perbankan syariah. Disisi lain loyalitas nasabah juga menunjukkan loyalitas jangka panjang dan keterikatan pelanggan dengan Lembaga keuangan Islam. Dengan kepercayaan dan loyalitas yang kuat, lembaga keuangan syariah dapat menciptakan lingkungan yang kondusif bagi nasabah untuk merasa aman dan percaya diri dalam melakukan transaksi keuangan sesuai dengan prinsip syariah. Selain itu, kepercayaan dan loyalitas nasabah dapat secara positif mempengaruhi citra dan reputasi lembaga keuangan syariah, menarik calon nasabah baru dan mendukung pertumbuhan ekonomi berbasis syariah yang lebih luas. Oleh karena itu, menjaga dan memperkuat kepercayaan dan loyalitas nasabah menjadi prioritas Lembaga keuangan syariah untuk memastikan kelangsungan dan keberhasilannya dalam membangun ekosistem perbankan syariah yang berkelanjutan.⁶

Terlepas dari dampak positif dan resiko keamanan dari *penggunaan Mobile Banking* di dunia perbankan ada juga dampak negatif yang kita dapatkan apabila menggunakan sistem *Mobile Banking* yang tidak bisa kita hindari lagi, seiring dengan berkembangnya teknologi Internet yang dapat memudahkan segalanya juga banyak menimbulkan kejahatan yang biasa disebut dengan *CyberCrime*.

⁵ Amarta, "Pengaruh Teknologi Digital Dalam Perkembangan Layanan Perbankan Syariah." *Jurnal Ilmiah Research and Development Student (JIS)* vol.2. 2024, <https://doi.org/10.59024/jise.v2i3.788>

⁶ Jasman j. Ma'ruf, *Manajemen Perspektif Indonesia* (Aceh: USK Press, 2025).

Data CPR tahun 2022 menunjukkan tingginya frekuensi serangan siber terhadap sektor perbankan, dengan sekitar 1.113 serangan setiap minggu secara global. Hal inimenyoroti urgensi perlunya menangani masalah keamanan di sektor perbankan dengan cepat di masa depan. Selain itu, data dari Kementerian Komunikasi dan Informatika (Kominfo) menunjukkan bahwa dari tahun 2017-2022 tercatat 486.000 laporan kejahatan terkait informasi dan transaksi elektronik dengan mayoritas tindak penipuan transaksi online. Berbagai jenis penipuan siber, seperti *malware*, *phishing*, *voicephishing* dan *smishing*, juga menjadi ancaman yang kerap mengintai masyarakat dalam konteks keamanan digital.⁷

Salah satu ancaman terkini adalah serangan siber yang dilakukan oleh peretas yang mahir. Peretas dapat menggunakan berbagai metode seperti *phishing*, serangan *malware*, dan pencurian identitas untuk mengakses data nasabah dan merusak sistem perbankan. Serangan *phishing* melibatkan penipuan melalui email atau situs web palsu yang mengecoh nasabah untuk mengungkapkan informasi pribadi atau keuangan. Serangan *malware*, seperti *ransomware*, dapat menginfeksi sistem dan mengenkripsi data sehingga nasabah atau bank harus membayar tebusan untuk mendapatkan akses kembali. Pencurian identitas juga menjadi ancaman serius, dimana peretas mencuri identitas nasabah dan menggunakannya untuk melakukan kegiatan ilegal atau penipuan.⁸

Pencurian data di dunia online dikenal dengan istilah *phishing*, yang

⁷ Frygyta Dwi Sulistyany Kemal Idris Balaka, Aulia Rahman Hakim, "Pencurian Informasi Nasabah Di Sektor Perbankan.," *Yustitiabelen* 10, No. 3 (2024): 105–30, <https://doi.org/10.36563/Yustitiabelen.V10i2.1167>.

⁸ Muhazzab Alief Faizal et al., "Analisis Risiko Teknologi Informasi Pada Bank Syariah: Identifikasi Ancaman Dan Tantangan Terkini," *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam* 5, no. 2 (2023): 87–100, <https://doi.org/10.47435/asy-syarikah.v5i2.2022>.

merupakan kejahatan untuk memperoleh informasi pribadi atau rahasia seseorang secara ilegal. Tindakan ini bertujuan untuk memperoleh nomor kartu kredit, PIN, User ID, nomor telepon, nomor rekening, dan informasi pribadi lainnya. Salah satu metode yang digunakan oleh pelaku *phishing* adalah dengan menyebarkan tautan palsu di akun media sosial melalui iklan yang menarik dan menggiurkan. Dengan cara ini, pelaku dapat mencuri informasi pribadi dari orang tersebut untuk mendapatkan keuntungan, misalnya dengan mencuri uang dari rekening pengguna atau menggunakan rekening tersebut sebagai media pembayaran online. Kejadian pelanggaran privasi yang melibatkan bocornya informasi pribadi sering terjadi di Indonesia. Dalam sektor perbankan, informasi pribadi dapat terungkap dalam berbagai kegiatan seperti pertukaran data pribadi antara lembaga keuangan, penyaluran informasi kepada pihak ketiga terkait transaksi keuangan, atau melalui penyedia jasa pihak ketiga yang mengelola data transaksi.⁹

Dilansir dari laman website BPKN (Badan Perlindungan Konsumen Nasional) dalam pertemuan yang dihadiri oleh Komisioner BPKN RI Dr. Megawati Simanjuntak bersama Asisten Ekonomi, Pembangunan dan Kesejahteraan Pemprov Sulsel Ichsan Mustari mengatakan bahwa ada 5.579 serangan *Phising* yang terjadi di Indonesia sepanjang kuartal II tahun 2022. Jumlah serangan *Phising* ini meningkat sekitar 41,52 persen dari kuartal I tahun 2022 sebanyak 3.942. Dari data tersebut, *e-Wallet* menjadi produk keuangan yang paling rentan kebocoran data. Di bawahnya ada rekening bank, internet *banking*, *Mobile Banking*, hingga ATM Bank. Ada beberapa cara kerja *Phising* yang marak

⁹ Muhammad Fadli, Dijan Widijowati, and Dwi Andayani, "Pencurian Data Pribadi Di Dunia Maya (Phising Cybercrime) Yang Ditinjau Dalam Perspektif Kriminologi," *Co-Value Jurnal Ekonomi Koperasi Dan Kewirausahaan* 14, no. 12 (2024).

terjadi.¹⁰

Tercatat, sebaran *Phising* paling banyak mengincar lembaga keuangan. Persentasenya mencapai 41%. Berikutnya, sebanyak 32% serangan *Phising* menyerang *e-commerce*. Lalu, sebanyak 21% serangan *Phising* mengincar media sosial. Sementara, hanya ada 6% serangan *Phising* yang mengincar pencurian data di game online dan akun aset kripto.¹¹

Rendahnya tingkat pengetahuan masyarakat juga turut menyumbang tingginya jumlah laporan *phishing*. Lebih jauh, fakta bahwa pelaku *phishing* kini dapat menggunakan banyak nama domain untuk meningkatkan jumlah pengaduan yang mereka terima menjadi pertimbangan lain. Faktor pengetahuan dan kesadaran pengguna terhadap ancaman serangan *phishing* juga didukung oleh Octo Iskandar, dalam artikel tersebut penulis meneliti mengenai pengetahuan pengguna untuk mengidentifikasi website *phishing*. Pengetahuan pengguna terhadap domain, link atau website palsu yang menyerupai aslinya sangat minim, sehingga pengguna tidak menyadari bahwa telah menggunakan situs palsu.¹² Didukung oleh pernyataan Vania Trisnawati dkk, faktor yang membuat pengguna menjadi korban serangan *phishing* adalah kurangnya pengetahuan korban mengenai informasi kejahatan phishing seperti halnya memdedakan nama domain yang resmi dengan yang palsu, selain itu pengguna tidak memperhatikan indikator

¹⁰ Badan Perlindungan Konsumen Nasional Republik Indonesia, “Kasus Phising Makin Marak, Bpknri Bahas Strategi Pencegahan Bareng Pemprov Sulsel,” *Trimbun Makassar*, N.D, 15 Februari 2023.

¹¹ Fadly Ariadi, Suhandi Saputra, And Anggreita Tiara Putri, “Sosialisasi Ancaman Dan Pencegahan Phishing Terhadap Pengguna Sosial Media Kepada Siswa / I,” *Jari: Jurnal Pengabdian Kepada Masyarakat Republik Indonesia* 1, No. 2 (2023): 10–15, <https://mypublikasi.com/index.php/jari>.

¹² Octo Iskandar, “Analisis Kejahatan Online Phishing Pada Masyarakat,” *Leuser: Jurnal Hukum Nusantara* 1, no. 2 (2024): 32–36, <https://journal.myrepublikcorp.com/index.php/leuser/article/view/85>.

keamanan browser. Pengguna tidak mengetahui strategi dalam menghadapi serangan *phishing*, tidak memberitahukan e-mail *phishing* yang diterima kepada pihak bank serta tidak mengetahui kebijakan bank tentang layanan perbankan online. Selain itu, seringkali pengguna menggunakan kata sandi yang sama pada semua layanan di internet, yang dapat meningkatkan risiko keamanan data bagi pengguna.¹³

Sejumlah lembaga keuangan di Indonesia telah mengalami insiden *cybercrime* yang berdampak signifikan terhadap kepercayaan masyarakat. Perbankan yang pernah mengalami *cybercrime* yaitu BSI sebanyak 15 juta data nasabah atau setara dengan 15 TB pada Mei 2023, Asuransi BRI LIFE sebanyak 2 juta data nasabah atau setara 250 GB pada Juli 2021, BPJS kesehatan Indonesia terkena pada tahun 2021 dengan kebocoran data nasabah sebanyak 279 juta data penduduk Indonesia bocor. Dari ketiga perusahaan yang mengalami *cybercrime* peneliti lebih memilih di BSI karena permasalahan yang sedang terjadi dan sedang banyak diberitakan di media sosial.¹⁴

Pelaku kejahatan daring bisa secara besar-besaran mengancam keuangan dan reputasi bank dan organisasi (keuangan) lainnya. Selain itu, hal itu berdampak pada hubungan antara citra organisasi dan kepercayaan yang dimiliki pelanggan dan pihak-pihak terkait lainnya dalam organisasi. Pemberitaan negatif yang dihasilkannya dapat menimbulkan beberapa masalah serius bagi organisasi ketika

¹³ Sandra Mutiara Tirta Vania Trisnawati, Edy Soesanto, "Kesadaran Korban Cyber Crime Dalam Kasus Phising," *Jurnal Ilmu Pendidikan* 1, No. 10 (2025), <https://jutepe-joln.net/index.php/jurperu/article/view/500>.

¹⁴ Wahyu Bunga Lestari, "Pengawasan Dan Perlindungan OJK Kepada BSI Terhadap Serangan Cyber Crime Prespektif UU No.21 Tahun 2011 Serta Maqasis As-Syariah (Studi Kasus Di OJK Solo)" (Salatiga : Universitas Islam Negeri (UIN) Salatiga, 2024).

mereka menjadi korban kejahatan daring. Oleh karena itu, prinsip kehati-hatian dalam pengelolaan data dan sistem keamanan menjadi sangat penting dalam memastikan bahwa organisasi keuangan tetap terlindungi dari ancaman yang terus berkembang.

Prinsip kehati-hatian sebagai salah satu prinsip dalam kegiatan usaha bank di Indonesia wajib diterapkan atau di laksanakan oleh bank. Prinsip kehati-hatian (*prudential principle*) tersebut mengharuskan pihak bank untuk selalu waspada dan hati-hati dalam menjalankan usahanya, dalam arti harus selalu konsisten dan taat dalam melaksanakan peraturan perundang-undangan dibidang perbankan berdasarkan profesionalisme dan itikad baik.¹⁵ Menurut Novia Galuh Rima Dona dkk, yang meneliti penerapan prinsip kehati-hatian dalam analisis pembiayaan di bank syariah. Penulis mengidentifikasi bahwa analisis berdasarkan prinsip 5C (*Character, Capacity, Capital, Collateral, dan Condition*), 7P (*Personality, Party, Purpose, Prospect, Payment, Profitability, dan Protection*), 3R (*Returns, Repayment, dan Risk*), dan 1S (*Shariah compliance*) diperlukan sebagai upaya penyaringan dalam penyaluran pembiayaan kepada masyarakat. Hal ini bertujuan untuk meminimalisir risiko dan memastikan kepatuhan terhadap prinsip syariah.¹⁶

Pentingnya penerapan prinsip kehati-hatian dalam menjalani kegiatan usaha suatu bank merupakan hal yang amatesensial dengan mengingat peran bank dimasyarakat sebagai suatu Lembaga intermediasi. Dengan perannya tersebut,

¹⁵ Endra Syaifuddin Ahmad Anugerah Puji Sakti, "Penerapan Prinsip Kehati-Hatian (Prudential Principle) Dalam Proses Pembiayaan Pada Bank Syariah Di Indonesia (Studi Kasus Bank Syariah Indonesia Kantor Cabang Mataram Nusa Tenggara Barat)," *Jurnal Risalah Kenotariatan* 4, no. 1 (2023), <https://doi.org/https://doi.org/10.29303/risalahkenotariatan.v4i1.96>.

¹⁶ Lidya Angreini Novia Galuh Rima Dona, Rafida, "Pelaksanaan Prinsip Kehati-Hatian Dalam Indonesia Kc Jambi Gatot Subroto," *Jurnal Ekonomica Sharia : Jurnal Pemikiran Dan Pengembangan Ekonomi Syariah* 8 (2023): 205–20, <https://doi.org/https://doi.org/10.36908/Esha.V8i2.589>.

industry yang amat sentral dalam rangka menjaga stabilitas perekonomian nasional sehingga berimplikasi kepada diperlakukannya industri bank sebagai salah satu industri yang diatur secara ketat (*highly regulated*).

Dari aspek perbankan, prinsip kehati-hatian dapat diterapkan melalui langkah pencegahan, salah satunya dengan penggunaan perangkat lunak anti-phishing yang mampu mendeteksi konten phishing pada situs web, email, maupun aplikasi sehingga dapat mencegah pengguna mengakses situs palsu. Sistem ini umumnya terintegrasi dengan peramban web dan klien email untuk menampilkan domain asli dari situs yang dikunjungi. Bank syariah sebagai bagian dari sistem perbankan di Indonesia juga tidak terlepas dari ancaman kejahatan siber tersebut, sehingga perlu menjaga kepercayaan nasabah dengan menjamin keamanan data serta dana yang disimpan. Upaya tersebut dapat diperkuat melalui adanya kepastian hukum yang melindungi hak dan kewajiban nasabah dalam menggunakan layanan perbankan syariah.

Berdasarkan latar belakang diatas, maka kiranya perlu dilakukan penelitian dengan judul **“Pengaruh Ancaman *Phising*, dan Prinsip Kehati- Hatian terhadap Tingkat Kepercayaan Nasabah Pengguna *Mobile Banking*.”**

B. Rumusan Masalah

Berdasarkan latar belakang di atas, adapun rumusan masalah penelitian ini adalah sebagai berikut:

1. Apakah ancaman *Phising* berpengaruh terhadap kepercayaan nasabah pengguna *Mobile Banking*?
2. Apakah prinsip kehati-hatian nasabah berpengaruh terhadap kepercayaan

nasabah pengguna *Mobile Banking*?

3. Apakah ancaman *Phising* dan prinsip kehati-hatian berpengaruh terhadap kepercayaan nasabah pengguna *Mobile Banking*?

C. Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Untuk menganalisis pengaruh ancaman *Phising* terhadap kepercayaan nasabah pengguna *Mobile Banking*?
2. Untuk menganalisis pengaruh prinsip kehati-hatian nasabah terhadap kepercayaan nasabah pengguna *Mobile Banking*?
3. Untuk menganalisis pengaruh ancaman *Phising* dan prinsip kehati-hatian terhadap kepercayaan nasabah pengguna *Mobile Banking*?

D. Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini baik berupa teoritis maupun praktis adalah sebagai berikut:

1. Manfaat Teoritis

Diharapkan dapat memberikan manfaat untuk referensi bagi pengembangan ilmu pada topik yang sama dengan penelitian ini dan juga dapat memberikan sumbangan berupa ilmu dan wawasan pengetahuan yang berkaitan dengan ekonomi, khususnya mengenai pengaruh tingkat pemahaman, kemudahan dan kepercayaan mahasiswa terhadap penggunaan *Mobile banking* yang ditinjau dalam perspektif ekonomi Islam. Juga dapat dijadikan sebagai bahan pertimbangan dalam penyusunan penelitian selanjutnya.

2. Manfaat Praktis

a) Bagi Penulis

Pada hasil penelitian ini, diharapkan dapat menjadi penambah pengetahuan dan wawasan, serta dapat menjadi pengalaman yang sangat berharga bagi penulis dalam melakukan pengembangan ilmu. Khususnya mengenai pengaruh ancaman *Phising* dan prinsip kehati-hatian terhadap nasabah pengguna *Mobile Banking*.

b) Bagi Instansi

Dalam hasil penelitian ini dapat menjadi rujukan perusahaan penerbit untuk mengetahui sejauh mana mahasiswa menggunakan produk yang mereka terbitkan, serta dapat memperbaiki kelemahan pada sistem yang mereka gunakan, agar dapat menarik minat masyarakat yang lebih luas.

c) Bagi Peneliti Selanjutnya

Penelitian ini juga dapat dijadikan sebagai referensi maupun bahan informasi, dimana ketika akan mengambil permasalahan serupa bagi pihak-pihak yang berkepentingan terkait, terkhusus dalam faktor pengaruh ancaman *Phising* dan prinsip kehati-hatian terhadappada nasabah pengguna *mobile banking*, dan juga penelitian ini dapat diharapkan menambah literatur serta wawasan ilmu.

BAB II

KAJIAN TEORI

A. Penelitian Terdahulu Yang Relevan

Ketika melakukan sebuah penelitian, peneliti perlu melakukan studi literatur terlebih dahulu untuk mengetahui perbandingan antara beberapa penelitian dengan tema yang sama. Adapun beberapa penelitian terdahulu yang menjadi landasan dan berkaitan dengan penelitian yang sedang dilakukan oleh peneliti adalah sebagai berikut:

1. Andi Siti Nurbaya Sari dengan judul penelitian “Pengaruh Prinsip Kehati-Hatian Terhadap Ancaman Situs *Phishing* Pada Nasabah Pengguna *Internet Banking* (Studi Kasus Pada Bank Syariah di Kota Palopo)” Jenis penelitian yang digunakan ialah Metode Kuantitatif. Penelitian ini menggunakan 30 sampel dengan menggunakan teknik penarikan *sampel non probability* yaitu sampel jenuh. Instrumen yang digunakan ialah angket (kuesioner). Data diolah dan dianalisis menggunakan regresi linear sederhana dengan menggunakan SPSS 22 *for windows*. Hasil penelitian diperoleh bahwa prinsip kehati-hatian berpengaruh positif terhadap ancaman situs *phishing* sebesar 36,2% dengan nilai t hitung (3,982) nilai t tabel (2,048) dengan tingkat signifikan $0,000 < 0,05$. Artinya variabel prinsip kehati-hatian secara parsial berpengaruh secara signifikan terhadap ancaman situs Phising pada *internet banking* di bank syariah Kota Palopo. Jadi dapat disimpulkan bahwa dengan adanya prinsip kehati-hatian bank dan bagi nasabah dapat mengurangi risiko terjadinya acaman situs *Phising* serta lebih terjaminnya keamanan data

nasabah pada *Mobile Banking* di bank syariah kota palopo¹⁷. Adapun persamaan pada penelitian ini yaitu variabel X (Prinsip kehati-hatian) dan membahas mengenai ancaman situs *Phising*. serta lokasi penelitian di Kota yang sama yaitu Kota Palopo Adapun perbedaan pada penelitian ini yaitu variabel Y (Tingkat Kepercayaan Nasabah).

2. Imelia Damai Agustina dkk dengan judul penelitian “Perlindungan Hukum Nasabah dari Kejahatan *Phising* dalam Layanan Perbankan Digital di Indonesia” Dalam penelitian ini menjelaskan bahwa digitalisasi sektor perbankan yang dipicu oleh Revolusi Industri 4.0 telah membawa dampak signifikan terhadap kemudahan transaksi keuangan melalui layanan perbankan digital. Namun, kemajuan ini juga membuka celah terhadap ancaman kejahatan siber, khususnya phishing, yang bertujuan mencuri data pribadi nasabah melalui situs atau pesan palsu. Artikel ini menganalisis ketentuan hukum yang relevan, termasuk UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), KUHP, serta peraturan OJK seperti POJK No. 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital. Metode penelitian normatif kualitatif digunakan untuk mengkaji perlindungan hukum terhadap nasabah sebagai korban phishing dan tanggung jawab perbankan dalam mencegah serta menangani ancaman ini. Artikel ini merekomendasikan penguatan keamanan sistem teknologi bank, edukasi literasi digital nasabah, serta penegakan hukum yang lebih efektif guna

¹⁷ Andi Siti Nurbaya Sari, “Pengaruh Prinsip Kehati-Hatian Terhadap Ancaman Situs Phising Pada Nasabah Pengguna Internet Banking (Studi Kasus Pada Bank Syariah Di Kota Palopo)” (Palopo: Institut Agama Islam Negeri Palopo, 2021).

menciptakan layanan perbankan digital yang aman dan terpercaya.¹⁸ Adapun persamaan penelitian ini yaitu terdapat pada kejahatan Phising pada nasabah Bank Syariah, adapun perbedaan pada penelitian ini yaitu variabel X yang lebih spesifik yaitu kejahatan situs Phising dan layanan perbankan digital.

3. Siswanto dan Milda Dwi Lenita dengan judul penelitian “Prinsip Kehati-hatian Nasabah Perbankan Dalam Menjaga Keamanan Bisnis Dari *Social Engineering Fraud*” Artikel ini menyoroti pentingnya penerapan prinsip kehati-hatian oleh nasabah perbankan untuk melindungi data pribadi dan bisnis dari ancaman *social engineering fraud*. Penulis menekankan bahwa baik pihak bank maupun nasabah memiliki tanggung jawab bersama dalam menerapkan prinsip kehati-hatian guna mencegah kejahatan tersebut. Adapun pendekatan yang digunakan adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*concelptual approach*) dengan analisis bahan hukum yang digunakan adalah analisis preskriptif yaitu untuk memberikan argumentasi atas hasil penelitian yang dilakukan Adapun pada titik ini nasabah perbankan harus menerapkan prinsip kehati-hatian untuk mengantisipasi *kejahatan social engineering fraud* dengan cara sebagai berikut; Selalu waspada membagikan data pribadi, Jangan sembarangan mendownload file, Waspada saat akan klik link, dan Jangan mudah percaya dengan orang yang baru dikenal. Penerapan prinsip kehati-hatian dalam konteks menjaga dari kejahatan *social engineering fraud* dalam dunia

¹⁸ Damai Agusthin Imelia, Christy Nada Dinda, And Ananda Putri Nadia, “Perlindungan Hukum Nasabah Dari Kejahatan Phising Dalam Layanan Perbankan Digital Di Indonesia,” *Depositi: Jurnal Publikasi Ilmu Hukum Ученые: Fakultas Hukum, Universitas Katolik Widya Karya Malang* 2, No. 4 (2024): 132–48.

perbankan adalah untuk melindungi data pribadi dan bisnis.¹⁹ Adapun persamaan pada penelitian ini yaitu membahas mengenai prinsip Kehati-hatian nasabah perbankan. Adapun perbedaan pada penelitian ini yaitu variabel Y (Tingkat Kepuasan Nasabah) dan lokasi penelitian.

4. Sahwa Aulia S dkk dengan judul penelitian “Pengaruh Kesadaran Sosial Dan Prinsip-Prinsip Terhadap Kepercayaan Nasabah Di Bank Syariah” Penelitian ini bertujuan untuk mengeksplorasi pengaruh Kesadaran Sosial dan Prinsip-Prinsip terhadap Kepercayaan Nasabah di Bank. Dengan melibatkan sampel sebanyak 102 responden, penelitian ini menerapkan analisis struktural dan model pengukuran untuk menguji hipotesis serta memeriksa validitas dan konsistensi model. Hasil analisis menunjukkan bahwa Kesadaran Sosial memiliki dampak positif dan signifikan terhadap Kepercayaan Nasabah, dengan peran mediasi Prinsip-Prinsip. Prinsip-Prinsip juga terbukti memberikan kontribusi positif yang signifikan terhadap Kepercayaan Nasabah di Bank. Namun, terdapat beberapa aspek yang perlu diperhatikan dalam model pengukuran, termasuk evaluasi lebih lanjut terhadap validitas dan reliabilitasnya. Saran untuk pengembangan lebih lanjut mencakup penguatan edukasi Kesadaran Sosial dan Prinsip-Prinsip, implementasi kebijakan internal yang konsisten, peningkatan keterlibatan nasabah melalui program partisipasi sosial, peninjauan ulang model pengukuran, dan evaluasi serta perbaikan fit statistik. Penelitian ini memberikan wawasan yang berguna bagi bank Bri dalam meningkatkan hubungan dengan nasabah dan memperkuat

¹⁹ D W I Lenita Milda, “Prinsip Kehati-Hatian Nasabah Perbankan Dalam Menjaga Keamanan Bisnis Dari Social Engineering Fraudud,” *Justitiable-Jurnal Hukum Vpcedumenu: Universitas Bojonegoro* 7, No. 1 (2024): 82–100.

posisinya sebagai lembaga keuangan yang sesuai dengan nilai-nilai sosial.²⁰ Adapun persamaan pada penelitian ini yaitu variabel X2 (Prinsip kehati-hatian) dan variabel Y (Tingkat Kepercayaan Nasabah) pada bank syariah. Adapun perbedaan pada penelitian ini yaitu pada variabel X1 dan Lokasi penelitian

5. Zamzami Akromi Lubis dan Fauzi Arif Lubis dengan judul penelitian “Pengaruh Persepsi Keamanan dan Kepercayaan Terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber di Bank Syariah Indonesia” Tujuan dari penelitian ini adalah untuk mengetahui pengaruh Persepsi Keamanan dan Kepercayaan terhadap Loyalitas Nasabah Pada Bank Syariah Indonesia di Kota Medan, penelitian ini dilakukan pada Nasabah Bank Syariah. Jenis penelitian yang digunakan adalah penelitian kuantitatif. Pengambilan sampel menggunakan teknik sampling jenuh, karena peneliti hanya mengambil sampel responden karyawan yang berjumlah 97 responden. Teknik pengumpulan data menggunakan kuesioner yang telah diuji validitas dan reliabilitasnya. Teknik analisis data yang digunakan untuk menjawab hipotesis adalah regresi berganda, uji asumsi klasik, uji hipotesis F, uji hipotesis t, koefisien determinasi Studi ini meneliti dampak persepsi keamanan dan kepercayaan terhadap loyalitas nasabah setelah terjadinya serangan siber, termasuk insiden *phishing*. Hasil penelitian menunjukkan bahwa baik persepsi keamanan maupun kepercayaan memiliki pengaruh signifikan terhadap loyalitas nasabah. Ini menekankan pentingnya bank dalam

²⁰ Halim Usman Sahwa Aulia S, Antong, “Pengaruh Kesadaran Sosial Dan Prinsip-Prinsip Terhadap Kepercayaan Nasabah Di Bank Syariah,” *Journal of Economics, Business and Accounting* 7, no. 6 (2024).

memastikan keamanan sistem mereka untuk mempertahankan kepercayaan dan loyalitas nasabah.²¹ Adapun persamaan dalam penelitian ini yaitu membahas mengenai kasus *cybercrime* termasuk *Phising* terhadap loyalitas nasabah, penelitian ini dapat menambah referensi yang sejalan. Adapun perbedaan pada penelitian ini yaitu variabel dan lokasi penelitian.

B. Landasan Teori

1. Situs *Phising*

Meningkatnya angka kejahatan di seluruh dunia seiring dengan kemajuan teknologi. Sehingga berbagai risiko yang ada saat ini juga dapat disebabkan oleh komputer. Media sosial merupakan platform yang memudahkan koneksi jarak jauh dan pencarian informasi yang cepat. Mayoritas masyarakat di dunia memanfaatkan media sosial. Oleh karena itu, para pegiat kejahatan dunia maya memanfaatkan kesempatan ini untuk menyasar pengguna media sosial dengan berbagai aksinya. Kemudian mereka melancarkan serangan dengan berbagai teknik, termasuk phishing.

Tujuan utama *Phising* adalah mencuri identitas target atau mendapatkan akses ilegal ke akun seseorang. Dengan informasi yang dimiliki pelaku *Phising*, pelaku dapat melakukan berbagai jenis penipuan, seperti pencurian identitas, pencucian uang, atau serangan terhadap komputer dan sistem jaringan.²² Sebagian besar agama melarang keras tindakan penipuan dan pemalsuan. Misalnya, dalam Islam, terdapat larangan untuk memakan harta orang lain dengan jalan yang batil

²¹ Zamzami Akromi Lubis and Fauzi Arif Lubis, "Pengaruh Persepsi Keamanan Dan Kepercayaan Terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber Di Bank Syariah Indonesia," *El-Mal: Jurnal Kajian Ekonomi & Bisnis Islam* 5, no. 10 (2024): 4215–30.

²² Mochammad Mukti Ali Yoyo Sudaryo, Ferry Kosadi, *Sistem Informasi Manajemen Berbasis Artificial Intelligence Dan E-Business System* (Yogyakarta: Penerbit Andi, 2024).

(QS. Al-Baqarah:188).²³

وَلَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ وَتُدْخِلُوا بِهَا إِلَى الْحُكَّامِ لِتَأْكُلُوا فَرِيقًا مِّنْ أَمْوَالِ النَّاسِ بِالْإِثْمِ وَأَنْتُمْ تَعْلَمُونَ ۝

Terejamahnya:

“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.”

a. Pengertian Situs *Phising*

Istilah “*phishing*” berasal dari kata “*fishing*” yang dipelesetkan. Namun jelas istilah ini tidak berbanding aktivitasnya dengan nelayan. Dengan kata lain phiser tidak memancing ikan. *Phiser* yang online akan lebih senang memancing informasi yang berharga. Secara definisi, phishing adalah Upaya mencuri data sensitif dengan menipu seseorang untuk memberikan kata sandia tau data kartu kredit, atau mengunduh virus komputer.²⁴ Ini adalah kerugian ganda, karena korban kehilangan data dan uang mereka.

Phishing adalah tindakan meminta (memancing) pengguna komputer untuk mengungkapkan informasi rahasia dengan cara mengirimkan pesan penting palsu, dapat berupa e-mail, website, atau komunikasi elektronik lainnya. Pesan palsu tersebut tampak seperti sungguhan dan meminta korban untuk segera mengirimkan informasi tertentu, biasanya diikuti dengan ancaman jika tidak mengirimkan informasi tersebut maka akan mengalami konsekuensi buruk.²⁵

Phishing termasuk dalam kejahatan *cybercrime*, dimana sekarang ini

²³ Lajnah Pentashihan Mushaf Al-Qur’an, *Qur’an Kemenag* (Indonesia, 2022).

²⁴ Febriansyah Fery, *Cybercrime : Kejahatan Di Balik Layar Digital* (Ponorogo: Najaha, 2025).

²⁵ Edy Santoso, *Hukum Siber: Permasalahan Hukum Bisnis Di Bidang Teknologi Informasi Dan Komunikasi* (Jakarta: Prenada Media, 2023).

marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer. Bagi *hacker* cara ini merupakan cara paling mudah untuk di jadikan serangan. Meskipun di anggap mudah dan sepele tapi tetap saja ada pengguna yang masuk ke perangkap sang hacker.²⁶

Berdasarkan pengertian *Phising* diatas maka dapat di simpulkan bahwa orang-orang yang bertransaksi secara daring melalui situs web perbankan biasanya menjadi sasaran kejahatan ini. Caranya dengan membuat email palsu yang sangat mirip dengan email asli bank. Karena sangat mirip dengan email asli, isi email palsu tersebut biasanya cukup meyakinkan. Agar mereka yang tertipu untuk mengunjungi situs web palsu tersebut. Setelah mengakses situs web palsu tersebut, korban niscaya akan mulai memberikan informasi pribadi dan rincian keuangan pada formulir informasi tersebut. Dengan demikian, materi tertulis tersebut sudah mulai muncul di basis data pelaku. Akibatnya, pelaku memiliki kendali penuh atas pemindahan informasi apa pun dari akun korban ke akunnya sendiri.

b. Indikator Ancaman Situs *Phising*

Situs *phishing* dirancang untuk menipu pengguna agar memberikan informasi sensitif seperti kredensial login, data kartu kredit, atau informasi pribadi lainnya. Berikut ini indikator yang menyebabkan adanya bahaya *Phising*:²⁷

²⁶ Fery, *Cybercrime : Kejahatan Di Balik Layar Digital*.

²⁷ Efy Zam, *Phising: Cara Mudah Menyadap Password & Pencegahannya* (Jakarta Selatan: MediaKita, 2023).

1) Rendahnya pengetahuan

Terjadinya *Phising* bisa disebabkan karena kelalaian manusia berupa kurang telitian dan rendahnya pengetahuan akan teknologi keamanan sehingga mudah dibobol oleh pelaku kejahatan.

2) Logika dan kepercayaan

Secara psikologis, pengguna sering kali memiliki rasa percaya yang tinggi terhadap pesan atau informasi yang tampak berasal dari sumber yang mereka kenal, termasuk teman, keluarga, atau akun resmi bank di media sosial dan mengabaikan logika dari dalam pikirannya. Penyerang memanfaatkan kepercayaan ini dengan menggunakan teknik rekayasa sosial (*social engineering*) untuk menipu korban agar memberikan informasi pribadi mereka. Karena terpancing dengan rasa takut, kepanikan, atau urgensi palsu sering dimanfaatkan dalam modus *phishing*, misalnya dengan pesan yang mengklaim adanya aktivitas mencurigakan di akun bank pengguna atau ancaman pemblokiran rekening jika tidak segera mengambil tindakan. Ketika pengguna merasa tertekan atau terburu-buru, mereka lebih cenderung mengabaikan langkah-langkah verifikasi keamanan, seperti memeriksa keaslian tautan atau situs yang mereka kunjungi.

c. Dampak Kejahatan *Phising*

Dampak dari *phishing* tidak hanya merugikan individu, tetapi juga dapat menimbulkan konsekuensi serius bagi perusahaan dan organisasi, termasuk kebocoran data, kerugian finansial, hingga rusaknya reputasi. Oleh karena itu, pemahaman mengenai dampak kejahatan *phishing* sangat penting agar masyarakat dapat lebih waspada dan menerapkan langkah-langkah pencegahan yang efektif.

Berikut ini beberapa dampak psikologis yang bisa ditimbulkan oleh *Phising* yaitu sebagai berikut:²⁸

- 1) Stres. Korban *Phising* bisa merasa stress karena khawatir data pribadi mereka disalahgunakan oleh pelaku, atau karena mendapat tekanan dari pihak-pihak yang terkait dengan data yang dicuri seperti bank, Perusahaan, atau instansi pemerintah.
- 2) Trauma. Korban kejahatan ini bisa mengalami trauma yang membuat mereka takut atau ragu untuk menggunakan layanan online lagi, seperti berbelanja online, bertransaksi online, atau berkomunikasi online.
- 3) Depresi. Korban kejahatan ini bisa mengalami depresi karena merasa malu, bersalah, atau rendah diri akibat menjadi korban penipuan online.
- 4) Kecemasan. Korban kejahatan ini bisa mengalami kecemasan karena tidak tahu bagaimana cara mengatasi masalah yang ditimbulkan oleh *Phising*, atau karena khawatir akan menjadi korban *Phising* lagi di masa depan

d. Pencegahan dan Perlindungan dari Serangan *Phising*

Dengan adanya serangan *phishing* membuat semua masyarakat resah dan harus berhati-hati lagi. Berikut tips pencegahan dan perlindungan dari serangan *phishing* yang bisa kami berikan agar anda, keluarga, dan organisasi anda tetap aman.²⁹

1) Kesadaran Pengguna

- a) Tingkatkan kesadaran pengguna tentang serangan phishing, seperti cara

²⁸ Lisangan Nisa, Lazarusli, Pribadi, Marzuki, *Keamanan Siber (Cyber Security)* (Padang: CV. Gita Lentera, 2025).

²⁹ Edy Santoso, *Hukum Siber: Permasalahan Hukum Bisnis Di Bidang Teknologi Informasi Dan Komunikasi* (Jakarta: Prenada Media, 2023).

membedakan email, pesan, atau situs web yang mencurigakan.

- b) Pelajari pengguna tentang cara menjaga keamanan online, seperti menghindari mengklik tautan atau lampiran yang mencurigakan, memberikan login atau data pribadi secara sembarangan, dan tidak berbagi data pribadi melalui email atau pesan yang tidak terenkripsi.

2) Pendidikan dan Pelatihan

Berikan pelatihan rutin kepada karyawan tentang serangan *phishing* dan strategi yang digunakan oleh penyerang. Simulasikan serangan dengan alat pelatihan yang memungkinkan karyawan untuk mengenali dan melaporkan serangan tersebut. Berikan panduan yang jelas tentang tindakan yang harus diambil jika seseorang mencurigai serangan *phishing*.

3) Verifikasi Identitas Anda

- a) Sebelum memberikan informasi sensitif, pastikan Anda mengetahui siapa orang yang memintanya melalui email, pesan, atau telepon
- b) Untuk melindungi akun online Anda, gunakan metode otentikasi kuat seperti verifikasi dua faktor (2FA).

4) Penyeleksi Email

- a) Gunakan program keamanan email yang dapat mengidentifikasi dan memfilter email phishing sebelum mencapai kotak masuk pengguna.
- b) Perbaiki sistem perlindungan email secara berkala.

5) Keamanan dan Pembaruan Perangkat Lunak

- a) Selalu memperbarui perangkat lunak sistem operasi, browser web, aplikasi, dan program keamanan dengan patch keamanan terbaru.

b) Aktifkan fitur pembaruan otomatis untuk memastikan perangkat selalu memiliki perlindungan terbaru.

6) Anti Virus dan Firewall

Untuk melindungi sistem dari serangan phishing dan malware, aktifkan dan perbarui firewall dan program antivirus.

7) Lihat Situs Web

Sebelum memberikan data pribadi atau melakukan transaksi online, pastikan situs web aman. Ini dapat dilihat dengan melihat tanda ikatan keamanan dan tanda kunci keamanan pada alamat URL (<https://>).

Ancaman *phishing* di dunia digital semakin serius seiring perkembangan teknologi yang pesat. Penyerang *phishing* terus mengembangkan metode mereka untuk mencuri informasi pribadi pengguna yang dapat digunakan untuk tujuan jahat. Penting bagi kita untuk tetap waspada, menggunakan langkah-langkah keamanan yang tepat, dan meningkatkan kesadaran tentang *phishing*. Dengan melakukan langkah-langkah pencegahan yang diperlukan, kita dapat melindungi diri kita sendiri dan melawan upaya penipuan online ini

e. Teknik dan Metode *Phishing* dalam *CyberCrime*

Berbagai teknik dan metode *phishing* terus berkembang seiring dengan kemajuan teknologi dan semakin canggihnya upaya para pelaku kejahatan siber. Beberapa metode yang umum digunakan antara lain *spear phishing* (serangan yang ditargetkan pada individu atau organisasi tertentu), *whaling* (menargetkan eksekutif atau pejabat tinggi), *smishing* (*phishing* melalui pesan teks), serta *vishing* (*phishing* melalui panggilan suara). Pemahaman tentang teknik dan

metode *phishing* sangat penting bagi individu maupun organisasi agar dapat mengenali, mengantisipasi, dan menghindari serangan siber yang berpotensi merugikan. Dengan meningkatkan kesadaran akan ancaman ini, masyarakat dapat lebih waspada dalam melindungi data dan informasi pribadi mereka dari penyalahgunaan. Teknik atau cara kerja *Phising* secara umum tersebut dijabarkan sebagai berikut:³⁰

1) *Spear Phishing*

Spear phishing adalah jenis serangan *phishing* yang sangat menyesuaikan dan menargetkan orang-orang tertentu. Dalam *spear phishing*, penyerang melakukan pengintaian pada target, baik individu atau organisasi, untuk memberikan informasi yang tampak asli dan kredibel. Serangan seperti ini biasanya ditujukan kepada mereka yang memiliki akses ke informasi penting atau yang memiliki pengetahuan orang dalam tentang organisasi tertentu.

2) *Whaling Phishing*

Whaling Phishing adalah jenis serangan siber yang menargetkan individu atau karyawan bernilai tinggi di dalam suatu organisasi. Ini adalah jenis *phishing* yang lebih canggih dan ditargetkan di mana penyerang menargetkan korban dan menggunakan taktik untuk mengambil keuntungan dari posisi kelemahan korban.

3) *Smishing Phishing*

Smishing Phishing adalah teknik yang digunakan untuk menggambarkan serangan *phishing* yang menggunakan pesan teks (SMS) sebagai sarana untuk mengidentifikasi target. Pelaku *smishing* memancing korban agar memberikan

³⁰ R Mcdonough, *Cyber Smart: Five Habits To Protect Your Family, Money, And Identity From Cyber Criminals* (Canada: Wiley, 2023).

informasi pribadi atau mengunjungi situs web palsu, atau mengirimkan pesan teks palsu yang terlihat seperti pesan resmi dari lembaga atau perusahaan terpercaya

4) *Vishing Phising*

Vishing (Voice Phishing) adalah jenis serangan *phishing* yang menggunakan telepon panggilan untuk mengelabui korban agar memberikan informasi pribadi atau uang. Pelaku *phishing* sering menyamar sebagai perwakilan dari lembaga keuangan, bank, atau bisnis lain yang sah untuk mendapatkan kepercayaan klien.

f. Teknik Manipulasi Sosial Pelaku *Phising*

Phishing adalah metode penipuan di dunia maya di mana pelaku berusaha memperoleh informasi sensitif, seperti kata sandi dan data kartu kredit, dengan menyamar sebagai entitas terpercaya. Berikut ini adalah beberapa teknik manipulasi sosial yang sering digunakan oleh penyerang *phishing*:³¹

- 1) Penipuan Identitas, juga dikenal sebagai *spoofing*: Penyerang *Phising* sering menggunakan metode *spoofing* untuk menyamarkan atau memalsukan identitas mereka. Mereka dapat menipu alamat email, nama pengirim, atau header email sehingga terlihat seolah-olah pesan tersebut berasal dari sumber yang terpercaya, seperti bank atau perusahaan terkemuka.
- 2) Tekanan Waktu (*Urgency*): Penyerang *Phising* seringkali membuat korbannya tertekan dengan mengirimkan pesan yang menekankan urgensi. Untuk membuat korban panik dan mengabaikan peringatan, mereka menggunakan kata-kata seperti “tindakan segera diperlukan” atau “akun Anda akan dinonaktifkan.”.

³¹ Annisa Yuswanita Et Al., *Keamanan Informasi: Jenis, Prinsip Dan Implementasi Dalam Era Digital* (Sumatera Barat: Fahmi Karya, 2025).

- 3) Sosial Rekayasa (*Social Engineering*): Penyerang *Phising* menggunakan sosial rekayasa sebagai teknik manipulasi psikologis untuk memanipulasi korbannya. Untuk mendapatkan kepercayaan korban dan meminta informasi pribadi atau rahasia, mereka dapat berpura-pura menjadi anggota tim dukungan pelanggan, mitra bisnis, atau teman yang dikenal.
- 4) Manipulasi Emosi: Penyerang *Phising* sering mencoba mengendalikan perasaan korban untuk mendapatkan reaksi yang diinginkan. Mereka dapat memaksa korban untuk melakukan tindakan yang diminta, seperti mengklik tautan berbahaya atau membuka lampiran berbahaya, dengan menggunakan ancaman, kerentanan emosional, atau imbalan palsu.
- 5) Pemalsuan Situs Web (*Pharming*): Pembajakan atau pemalsuan situs web yang sah adalah teknik *Phising* yang dikenal sebagai “*pharming*.” Dengan mengarahkan korbannya ke situs web palsu yang terlihat seperti situs web asli, penyerang berusaha mencuri data masuk atau membuat korban mengungkapkan informasi pribadi.
- 6) Pengalihan Perhatian (*Distraction*): Penyerang *Phising* dapat menggunakan teknik pengalihan perhatian untuk mengalihkan perhatian korban dari tanda-tanda peringatan. Ini dapat mencakup informasi atau penawaran yang menarik untuk membuat korban fokus pada hal tersebut daripada mengabaikan ketidaksesuaian atau kejanggalan lainnya.
- 7) *Pretexting*: Teknik manipulasi sosial di mana penyerang *phishing* membuat skenario atau alasan yang tidak masuk akal untuk mendapatkan informasi dari korban. Untuk meyakinkan korban bahwa mereka membutuhkan informasi

pribadi atau akses ke akun korban, mereka dapat mengaku sebagai anggota tim internal perusahaan, penyedia layanan, atau pihak otoritas.

- 8) Penggunaan Logos atau Tampilan Merek Palsu: Penyerang *phishing* sering menggunakan logo, ikon, atau tampilan merek palsu dalam pesan atau situs web mereka untuk memberi kesan bahwa mereka adalah asli, sehingga pengguna dapat mengenali merek tersebut dan memberikan informasi tanpa mencurigai bahwa pesan atau situs web tersebut adalah asli.
- 9) Teknik Persuasif: Penyerang *phishing* menggunakan taktik persuasif yang kuat untuk meyakinkan korban untuk mengikuti instruksi yang diminta. Mereka dapat menggunakan imbalan palsu, penawaran menarik, atau janji hadiah untuk menarik korban untuk memberikan informasi sensitif atau melakukan tindakan tertentu.
- 10) *Phishing* Melalui Media Sosial: Penyerang *phishing* juga menggunakan media sosial untuk melakukan serangan mereka. Mereka dapat membuat akun palsu atau mencuri akun yang sudah ada untuk mempengaruhi dan memanipulasi pengguna media sosial. Memposting tautan berbahaya di profil atau grup atau mengirim pesan pribadi yang tampak asli adalah beberapa contoh teknik ini.

Mengenali beberapa Teknik di atas dapat membantu individu lebih waspada terhadap upaya *phishing* dan mengambil langkah pencegahan yang tepat untuk melindungi informasi pribadi mereka.

2. Prinsip Kehati-hatian

a. Pengertian Prinsip Kehati-hatian

Pengertian Prinsip Kehati-Hatian Prinsip Kehati-hatian berasal dari kata “hati-hati” (*prudent*) yang erat kaitannya dengan fungsi pengawasan bank dan manajemen bank. *Prudent* dapat juga diterjemahkan dengan bijaksana, namun dalam dunia perbankan istilah itu digunakan dan diterjemahkan dengan hati-hati atau kehati-hatian.³²

Prinsip kehati-hatian adalah suatu prinsip yang menyatakan bahwa bank dalam menjalankan fungsi dan kegiatan usahanya wajib menerapkan prinsip kehati-hatian dalam rangka melindungi dana masyarakat yang dipercayakan kepadanya.³³

Jadi, dalam rangka menjaga dana masyarakat yang dipercayakan kepada bank, asas kehati-hatian perbankan mengamanatkan agar bank dan lembaga lainnya menjalankan kegiatan operasionalnya dengan mengenali nasabahnya dan mengantisipasi terus tingginya kepercayaan masyarakat terhadap lembaga keuangan. Pendekatan ini mendorong masyarakat untuk menyimpan uang di bank tanpa ragu atau bimbang.

b. Indikator Prinsip Kehati-hatian

Prinsip kehati-hatian dalam perbankan (*prudential banking principles*) bertujuan untuk memastikan stabilitas dan integritas sistem perbankan. Prinsip *Transparansi*, *Responsibility*, dan *Kewajaran* merupakan bagian dari *Good Corporate Governance* (GCG) dalam perbankan yang bertujuan untuk

³² Fachriah Et Al., *Hukum Lembaga Keuangan* (Pekan Baru: CV. Ekadanta Press, 2025).

³³ Eka Lestari, *Layanan Perbankan Fase F* (Medan: Umsu Press, 2024).

memastikan operasional yang adil, akuntabel, dan berkelanjutan. Berikut adalah penjelasan dari masing-masing prinsip beserta indikatornya³⁴.

- 1) *Transparency*, Transparansi dalam perbankan berarti bahwa bank harus memberikan informasi yang jelas, akurat, dan dapat diakses oleh pemangku kepentingan, termasuk nasabah, regulator, dan pemegang saham.
- 2) *Responsibility*, Prinsip tanggung jawab dalam perbankan mengacu pada kewajiban bank untuk mematuhi peraturan yang berlaku dan menjalankan operasional dengan etika serta tanggung jawab sosial.
- 3) *Fairness*, Prinsip kewajaran memastikan bahwa bank menjalankan usahanya dengan memperlakukan semua pihak secara adil, tanpa diskriminasi, dan sesuai dengan hak serta kewajiban yang berlaku.

Ketiga prinsip ini menjadi dasar dalam menjaga kepercayaan publik terhadap industri perbankan serta memastikan stabilitas sistem keuangan.

c. Landasan Prinsip Kehati-hatian

Penerapan prinsip kehati-hatian bank ini erat kaitannya dengan fungsi bank sebagai *agent of trust*, yaitu bank wajib menjaga kepentingan dan kepercayaan masyarakat dalam menjalankan kegiatan usahanya yang sebagian besar dananya berasal dari simpanan masyarakat. Pihak bank sendiri akan mau menempatkan atau menyalurkan dananya pada debitur atau masyarakat apabila dilandasi adanya unsur kepercayaan. Dibawah ini Al-Qu'ran Surat Al Hujarat Ayat 6, menjelaskan bahwa:³⁵

³⁴ Bambang Rianto Rustam, *Manajemen Risiko Perbankan Syariah Di Indonesia* (Jakarta: Penerbit Salemba, 2024).

³⁵ Lajnah Pentashihan Mushaf Al-Qur'an, *Qur'an Kemenag* (Indonesia, 2022)

يَا أَيُّهَا الَّذِينَ آمَنُوا إِنْ جَاءَكُمْ فَاسِقٌ بِنَبَأٍ فَتَبَيَّنُوا أَنْ تُصِيبُوا قَوْمًا بِجَهَالَةٍ فَتُصِحِّحُوا عَلَىٰ مَا فَعَلْتُمْ
لُدْمِينَ

Terjemahnya:

“Wahai orang-orang yang beriman, jika seorang fasik datang kepadamu membawa berita penting, maka telitilah kebenarannya agar kamu tidak mencelakakan suatu kaum karena ketidaktahuan(-mu) yang berakibat kamu menyesali perbuatanmu itu.

Ayat ini menekankan pentingnya kehati-hatian dalam menerima informasi, khususnya dari orang-orang yang tidak dapat dipercaya. Sebelum menerima berita, umat Islam disuruh untuk melakukan penelitian atau verifikasi, sehingga tidak salah dalam mengambil tindakan atau menyebarkan berita yang belum tentu benar.

3. Kepercayaan Nasabah

a. Pengertian Kepercayaan

Kepercayaan merupakan titik temu dari interaksi ekonomi dan sosial dimana ketidakpastian muncul dari interaksi tersebut. Kepercayaan pada dasarnya hanya diperlukan dalam situasi ketidakpastian itu muncul.³⁶

Penelitian Ring dan van de Ven dalam Yan Chen dkk, memberikan dua definisi umum kepercayaan di seluruh organisasi, yaitu kepercayaan diri atau kepastian dalam ekspektasi seseorang tentang perilaku orang lain dan kepercayaan pada niat baik orang lain.³⁷ Mc Allister dalam Nina Hasche mengemukakan bahwa dalam literatur kepercayaan interpersonal bahwa ada dua jenis kepercayaan, yaitu afektif dan kognitif.³⁸ Kepercayaan afektif didasarkan pada

³⁶ Astriyanti Et Al., *Kepuasan Nasabah Pada Lembaga Keuangan Non Bank* (Bali: Cv. Intelektual Manifes Media, 2023).

³⁷ Yan Chen et al., “The Influence of Trust on Creativity: A Review.,” *Frontiers in Psychology* 12 (2021): 706234, <https://doi.org/10.3389/fpsyg.2021.706234>.

³⁸ Nina Hasche et al., “Intra-Organizational Trust in Public Organizations – the Study of

perawatan dan kepedulian interpersonal timbal balik atau ikatan emosional, sedangkan kepercayaan kognitif didasarkan pada keyakinan individu tentang keandalan dan ketergantungan rekan sebaya serta kompetensi.

Perbankan syariah harus mampu menerapkan nilai-nilai ke-Islaman di dalam prosedur dan mekanisme kerjanya. Sehingga perbankan syariah dapat senantiasa berada dalam koridor nilai-nilai Islam guna mencapai pengembangan ke arah yang lebih baik lagi. Penerapan nilai-nilai Islam pada bank syariah secara baik dan benar tentu saja akan mempengaruhi keputusan masyarakat untuk menjadi nasabah bank syariah. Penerapan nilai-nilai Islam perlu menjadi perhatian penting bagi setiap bank syariah. Dengan penerapan nilai-nilai Islam, akan meningkatkan kepercayaan masyarakat untuk menempatkan dananya ataupun menggunakan pembiayaan dari perbankan syariah. Semakin banyak masyarakat menempatkan dananya atau menggunakan pembiayaan dari bank syariah, itu menunjukkan masyarakat telah menjadi nasabah yang loyal pada bank syariah.

Salah satu aspek yang tidak kalah penting untuk menjaga agar nasabah tetap loyal adalah kepercayaan. Pernyataan tersebut diperkuat dengan pendapat para ahli yang menyatakan bahwa kepercayaan merupakan salah satu unsur penting loyalitas nasabah, kepercayaan sebagai dasar penting untuk membangun dan memelihara hubungan jangka panjang. Kepercayaan merupakan modal penting dalam meningkatkan loyalitas nasabah terutama dalam menjaga hubungan jangka panjang, sehingga kepercayaan menjadi peran penting dalam keberlangsungan perusahaan untuk waktu yang akan datang.

b. Pentingnya Kepercayaan Pelanggan

Kepercayaan pelanggan pada produk dan perusahaan merupakan langkah yang baik bagi perusahaan. Kepercayaan pelanggan selain untuk basis konsumen dalam jangka panjang atau loyalitas, juga bagi perkembangan bisnis menjadi penting diantaranya, karena:³⁹

- 1) Tidak ada kepercayaan, maka tidak ada pelanggan Konsumen/pelanggan memiliki pilihan, mereka tidak akan berbelanja pada produk/perusahaan yang tidak mereka percaya. Ketika koneksi yang tulus dimiliki oleh perusahaan kepada pelanggannya, maka perusahaan akan menjadi pilihan pertama yang mereka ingat.
- 2) Berdampak langsung pada keuntungan perusahaan Hasil PwC's 2022 *Consumer Intelligence Series Survey on Trust*, diketahui bahwa 3% pelanggan telah membayar premi untuk sebuah perusahaan karena mereka mempercayai mereka. Dalam survei ini, sembilan dari 10 (91%) pelanggan menyatakan akan membeli dari perusahaan yang mereka percayai. Dari kelompok itu, 14% mengatakan mereka akan membeli lebih banyak secara signifikan.
- 3) Keunggulan Kompetitif Konsumen saat ini lebih sadar dengan siapa mereka berbisnis. Kesetiaan mereka telah melampaui siapa yang dapat menyajikan produk atau layanan terbaik dan beralih ke bisnis yang peduli dengan transparansi, autentik, dan berfokus pada membangun hubungan yang tulus daripada melakukan penjualan berikutnya. Inilah yang pada dasarnya akan

³⁹ Djoko Purwanto, *Komunikasi Bisnis*, 3rd Ed. (Jakarta: Erlangga, 2022).

membantu bisnis terus tumbuh dan berkembang bahkan di pasar yang kompetitif.

- 4) Reputasi Bisnis dengan reputasi yang sangat baik akan meningkatkan nilai yang dirasakan, menarik lebih banyak pelanggan, dan mendorongnya ke tingkat berikutnya. Dalam model bisnis ini, praktis satu-satunya jaminan yang dimiliki pelanggan bahwa dia dapat mempercayai produk dan layanan yang dijual kepadanya adalah reputasi umum merek itu sendiri. Ketika pelanggan mempercayai bisnis/produk atau jasa/layanan tertentu, mereka menganggap pilihan itu kredibel. Ini berarti advokasi, loyalitas, dan keterlibatan yang lebih besar dari pelanggan.

c. Kepercayaan Nasabah Bank Syariah

Kepercayaan merupakan salah satu kunci jangka Panjang untuk meningkatkan penjualan suatu produk. Kepercayaan juga sangat berpengaruh terhadap komitmen nasabah yang timbul karena keyakinan bahwa mitranya akan memberikan apa yang diharapkan. Nasabah yang percaya terhadap suatu Perusahaan berarti telah menaruh keyakinan yang tinggi pada Perusahaan yang membuat nasabah mempertahankan hubungannya dengan Perusahaan sehingga terjalin ikatan emosional yang kuat.⁴⁰

Berdirinya Bank syariah tentunya memiliki landasan atau dasar hukum yang melindungi dan menjadi dasar menjalankan segala aktivitas perekonomian yang meliputi kegiatan perbankan. Dalam berjalannya segala aktivitas perbankan, bank syariah memiliki dua dasar hukum berdasarkan peraturan negara dan

⁴⁰ Eka Wahyu Budianto, *Determinan Perilaku Nasabah Bank Syariah (2023-2025)* (malang: PT. Afanin Media Utama, 2025).

berdasarkan Al-Qur'an dan hukum Islam yang lainnya. Salah satu landasan hukum Islam tentang bank syariah adalah surat An-Nisa/4: 29.⁴¹

يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَأْكُلُوا أَمْوَالَكُمْ بَيْنَكُمْ بِالْبَاطِلِ إِلَّا أَنْ تَكُونَ تِجَارَةً عَنْ تَرَاضٍ مِّنْكُمْ وَلَا تَقْتُلُوا أَنْفُسَكُمْ إِنَّ اللَّهَ كَانَ بِكُمْ رَحِيمًا

Terjemahnya:

“Wahai orang-orang yang beriman, janganlah kamu memakan harta sesamamu dengan cara yang batil (tidak benar), kecuali berupa perniagaan atas dasar suka sama suka di antara kamu. Janganlah kamu membunuh dirimu. Sesungguhnya Allah adalah Maha Penyayang kepadamu.”

Dari ayat ini bisa diambil salah satu poin penting yakni menyampaikan amanat. Dalam bank syariah baik pihak Bank maupun nasabah harus menjaga amanah yang telah disepakati dalam akad sebelumnya hal ini bertujuan untuk menjaga kepercayaan dan tetap berkegiatan ekonomi tanpa kecurangan atau kebohongan sedikitpun.

Berdasarkan hal tersebut, dapat dikatakan bahwa kepercayaan merupakan pandangan yang dianut oleh orang-orang yang menganggap bahwa orang yang mereka percaya akan menyampaikan apa yang mereka yakini, dan kepercayaan suatu nasabah akan terbentuk jika mereka menerima layanan yang bermutu tinggi. Kebahagiaan nasabah juga sangat dipengaruhi oleh kepercayaan. Akibatnya, nasabah harus merasakan sendiri tingkat layanan yang ditawarkan oleh bank syariah agar dapat memperoleh kepercayaan mereka. Setelah itu, akan terbentuk suatu pertemuan yang menandai dimulainya terbentuknya kepercayaan, sehingga nasabah merasa puas dengan bank syariah tersebut.

⁴¹ Lajnah Pentashihan Mushaf Al-Qur'an, *Qur'an Kemenag* (Indonesia, 2022)

d. Indikator Kepercayaan

Kepercayaan nasabah berkembang secara bertahap dari waktu ke waktu, didasarkan pada pengalaman sebelumnya yang relevan, dan terbentuk dari waktu ke waktu. Kepercayaan nasabah sangat penting dalam industri perbankan karena dapat memperkuat ikatan antara nasabah dan pemberi pinjaman (pihak bank). Dasar dari setiap bisnis adalah kepercayaan dari para nasabahnya. Menciptakan dan mempertahankan nasabah memerlukan pengembangan kepercayaan mereka sehingga mereka merasa nyaman berbisnis dengan bank.

Berikut ini indikator kepercayaan pelanggan atau nasabah adalah sebagai berikut:⁴²

1) Kemampuan

Kepercayaan adalah ranah khusus, sehingga individu membutuhkan keyakinan akan seberapa baik seseorang memelihatkan performanya. Faktor pengalaman dan pembuktian performanya akan mendasari munculnya kepercayaan orang lain terhadap individu.

2) Integritas

Integritas terlihat dari konsistensi antara ucapan dan perbuatan dengan nilai-nilai diri seseorang. Kejujuran saja tidak cukup untuk menjelaskan tentang integritas, namun integritas memerlukan keteguhan hati dalam menerima tekanan.

3) Kebaikan Hati

Kebaikan hati berkaitan dengan intensi (niat). Ada ketertarikan dalam diri seseorang ketika berinteraksi dengan orang lain. Hal tersebut akan

⁴² Rahmadani Hidayat, Sarjon Defit, And Wardana, *Membangun Loyalitas Pelanggan Melalui Kepercayaan: Perspektif Manajemen Pemasaran* (Bali: Cv. Intelektual Manifes Media, 2025).

mengarahkannya untuk memikirkan orang tersebut dan memberikan intense untuk percaya atau tidak dengan orang tersebut.

Untuk itu Allah sangat melarang perbuatan khianat atas amanah karena akan menghilangkan kepercayaan pada diri seseorang. Orang yang berkhianat sebenarnya sadar dan mengetahui bahwa dirinya telah keluar dari kepercayaan yang diberikan atau diamanahkan sebelumnya. Surah Al Baqarah ayat 282 di bawah ini menjelaskan bahwa:⁴³

يَا أَيُّهَا الَّذِينَ آمَنُوا إِذَا تَدَايَنْتُمْ بِدِينٍ إِلَىٰ أَجَلٍ مُّسَمًّى فَاكْتُبُوهُ ۚ وَلْيَكْتُب بَيْنَكُمْ كَاتِبٌ بِالْعَدْلِ وَلَا يَأْب كَاتِبٌ أَنْ يَكْتُبَ كَمَا عَلَّمَهُ اللَّهُ فَلْيَكْتُبْ وَلْيُمْلِلِ الَّذِي عَلَيْهِ الْحَقُّ وَلْيَتَّقِ اللَّهَ رَبَّهُ وَلَا يَبْخَسْ مِنْهُ شَيْئًا فَإِنْ كَانَ الَّذِي عَلَيْهِ الْحَقُّ سَفِيهًا أَوْ ضَعِيفًا أَوْ لَا يَسْطِيعُ أَنْ يُمِلَّ هُوَ فَلْيُمْلِلْ وَلِيُّهُ بِالْعَدْلِ ۚ وَاسْتَشْهِدُوا شَهِيدَيْنِ مِنْ رَجَالِكُمْ فَإِنْ لَمْ يَكُونَا رَجُلَيْنِ فَرَجُلٌ وَامْرَأَتٌ مِمَّنْ تَرْضَوْنَ مِنَ الشُّهَدَاءِ أَنْ تَضِلَّ إِحْدَاهُمَا فَتُذَكِّرَ إِحْدَاهُمَا الْأُخْرَىٰ وَلَا يَأْب الشُّهَدَاءُ إِذَا مَا دُعُوا ۗ وَلَا تَسْمَعُوا أَنْ تَكْفُرُوا صَغِيرًا أَوْ كَبِيرًا إِلَىٰ أَجَلِهِ ۚ ذَلِكُمْ أَفْسَطُ عِنْدَ اللَّهِ وَأَقْوَمٌ لِلشَّهَادَةِ وَأَدْنَىٰ أَلَّا تَرْتَابُوا إِلَّا أَنْ تَكُونَ تِجَارَةً حَاضِرَةً تُدِيرُونَهَا بَيْنَكُمْ فَلَيْسَ عَلَيْكُمْ جُنَاحٌ أَلَّا تَكْتُبُوهَا وَأَشْهَدُوا إِذَا تَبَايَعْتُمْ ۗ وَلَا يُضَارَّ كَاتِبٌ وَلَا شَهِيدٌ ۗ وَإِنْ تَفَعَّلُوا فَإِنَّهُ فَسُوقٌ بِكُمْ ۗ وَاتَّقُوا اللَّهَ ۗ وَيُعَلِّمُكُمُ اللَّهُ ۗ وَاللَّهُ بِكُلِّ شَيْءٍ عَلِيمٌ

Terjemahnya:

“Wahai orang-orang yang beriman, apabila kamu berutang piutang untuk waktu yang ditentukan, hendaklah kamu mencatatnya. Hendaklah seorang pencatat di antara kamu menuliskannya dengan benar. Janganlah pencatat menolak untuk menuliskannya sebagaimana Allah telah mengajar-kan kepadanya. Hendaklah dia mencatat(-nya) dan orang yang berutang itu mendiktekan(-nya). Hendaklah dia bertakwa kepada Allah, Tuhannya, dan janganlah dia menguranginya sedikit pun. Jika yang berutang itu orang yang kurang akalnya, lemah (keadaannya), atau tidak mampu mendiktekan sendiri, hendaklah walinya mendiktekannya dengan benar. Mintalah kesaksian dua orang saksi laki-laki di antara kamu. Jika tidak ada (saksi) dua orang laki-laki, (boleh) seorang laki-laki dan dua orang perempuan di antara orang-orang yang kamu sukai dari para saksi (yang ada) sehingga jika salah seorang (saksi perempuan) lupa, yang lain mengingatkannya. Janganlah saksi-saksi itu menolak apabila dipanggil. Janganlah kamu bosan mencatatnya sampai batas waktunya, baik (utang itu) kecil maupun besar. Yang demikian itu lebih adil di sisi Allah, lebih dapat menguatkan

⁴³ Lajnah Pentashihan Mushaf Al-Qur'an, *Qur'an Kemenag* (Indonesia, 2022)

kesaksian, dan lebih mendekatkan kamu pada ketidakraguan, kecuali jika hal itu merupakan perniagaan tunai yang kamu jalankan di antara kamu. Maka, tidak ada dosa bagi kamu jika kamu tidak mencatatnya. Ambillah saksi apabila kamu berjual beli dan janganlah pencatat mempersulit (atau dipersulit), begitu juga saksi. Jika kamu melakukan (yang demikian), sesungguhnya hal itu suatu kefasikan padamu. Bertakwalah kepada Allah, Allah memberikan pengajaran kepadamu dan Allah Maha Mengetahui segala sesuatu.”

Dari penjelasan di atas, dapat diambil kesimpulan bahwa kepercayaan konsumen atau nasabah dapat terjalin apabila perusahaan tersebut memiliki reputasi produk atau jasa yang baik, selain itu keamanan dan kenyamanan dalam penggunaan produk dan jasa juga harus diperhatikan, manfaat dari produk dan jasa juga tak kalah penting untuk diperhatikan. Masyarakat cenderung lebih mempercayai layanan dengan produk ataupun jasa yang memiliki manfaat yang banyak atau dalam hal ini pada dunia perbankan.

4. *Mobile Banking*

a. *Pengertian Mobile Banking*

Mobile Banking merupakan salah satu layanan jasa perbankan yang memungkinkan nasabah untuk memperoleh informasi dan melakukan transaksi perbankan melalui jaringan internet.⁴⁴ *Mobile Banking* pada dasarnya merupakan gabungan dua istilah yaitu internet dan *banking* (bank).

Mobile Banking merupakan kegiatan perbankan yang memanfaatkan teknologi internet sebagai media untuk melakukan transaksi dan mendapatkan informasi lainnya melalui website milik bank. Kegiatan ini menggunakan jaringan internet sebagai perantara atau penghubung antara nasabah dengan bank tanpa harus mendatangi kantor bank. Nasabah dapat menggunakan perangkat komputer

⁴⁴ Rahmayati, *Sistem Informasi Manajemen Dan Keamanan Di Lembaga Keuangan Syariah* (Medan: Umsu Press, 2025).

desktop, laptop, tablet, atau *smartphone* yang terhubung ke jaringan internet sebagai penghubung antara perangkat nasabah dengan sistem bank.⁴⁵

b. Produk atau Jasa *Mobile Banking*

Mobile Banking adalah salah satu bentuk pelayanan yang diberikan oleh perbankan kepada nasabahnya untuk mempermudah para nasabah yang akan melakukan transaksi dengan tidak perlu datang ke bank karena kesibukannya, sehingga *Mobile Banking* saat ini banyak di gemari oleh nasabah yang memiliki aktivitas padat, sehingga di manapun mereka berada tetap dapat melakukan transaksi sehingga tidak perlu mengganggu aktivitasnya sedikitpun. Karena *Mobile Banking* hanya membutuhkan sedikit waktu untuk melakukan berbagai macam transaksi. Adapun beberapa indikator fitur layanan sebuah sistem *Mobile Banking* menurut Poon yaitu sebagai berikut:⁴⁶

- 1) Adanya akses informasi yang mudah mengenai jasa atau produk Fitur ini bisa memberi kemudahan para pemakai dalam melakukan akses informasi tentang produk ataupun jasa.
- 2) Tersedianya berbagai layanan transaksi Fitur yang disediakan memiliki keberagaman pada proses memberikan layanan pada para nasabah.
- 3) Tersedianya berbagai fitur Fitur layanan pada sistem informasi sebuah perbankan memiliki keberagaman Oleh karena itu bisa memberikan bantuan para nasabah dalam menjalankan transaksi
- 4) Adanya Inovasi Pada Produk Tersedianya berbagai fitur tambahan, oleh

⁴⁵ Titien Rahayuningsih, *Bank Dan Lembaga Keuangan Lainnya* (Sukoharjo: Epigraf Komunikata Prima, 2024).

⁴⁶ Wahyi Busyro Putri Jamilah, Eko Bagus Cahyo Purnomo, Muhammad Lisman, Rika Septianingsih, *Digital Banking* (Riau: Cv. Dotplus Publisher, 2025).

karena itu para nasabah merasa tertarik untuk memakai sistem internet banking dari sebuah bank

Jenis kegiatan yang terdapat pada *Mobile Banking* yaitu:⁴⁷

- 1) *Informational Mobile Banking* yaitu pelayanan jasa bank kepada nasabah dalam bentuk penyampaian berbagai informasi bank seperti program promosi bank, cara pembukaan rekening baru, kontak layanan nasabah, informasi tentang produk bank, informasi tingkat suku bunga bank, dan lain sebagainya, melalui jaringan internet dengan tidak melakukan eksekusi transaksi (*execution of transaction*).
- 2) *Communication Mobile Banking* yaitu pelayanan jasa bank kepada nasabah dalam bentuk interaksi komunikasi antara bank dengan nasabah secara terbatas seperti chatting, call center, dan lain sebagainya dengan tidak melakukan eksekusi transaksi.
- 3) *Transactional Mobile Banking* yaitu pelayanan jasa bank kepada nasabah untuk melakukan interaksi dengan pihak bank dengan melakukan eksekusi transaksi seperti pemindah bukuan (transfer), pembayaran tagihan, dan lain sebagainya.

c. Kelebihan dan Keuntungan *Mobile Banking*

Kelebihan dari *Mobile Banking* yaitu:⁴⁸

- 1) Transaksi perbankan dapat dilakukan kapan saja dan di mana saja.
- 2) *Mobile Banking* Muamalat dilengkapi dengan m Pass Code (*One Time Password*), yaitu SMS berisikan kode verifikasi transaksi yang dikirimkan ke

⁴⁷ Mohammad Rafi Hadzami, *Inovasi Dan Strategi Keuangan* (Yogyakarta: Deepublish, 2025).

⁴⁸ Rahayuningsih, *Bank Dan Lembaga Keuangan Lainnya*.

nomor ponsel nasabah yang telah terdaftar di bank.

Keuntungan menggunakan layanan *Mobile Banking* yaitu:

- 1) Hemat waktu, karena nasabah tidak perlu meninggalkan meja kerja untuk melakukan aktivitas perbankan, cukup menggunakan PC, Laptop atau smartphone yang telah terkoneksi dengan jaringan internet.
- 2) Aman, dilengkapi sistem keamanan berlapis dengan dukungan keamanan jaringan SSL (*Secure Socket Layer*).
- 3) Transaksi *Real Time Online*, karena dapat dilakukan kapanpun dan dimanapun melalui jaringan internet.
- 4) Satu akses untuk semua produk, dengan login hanya menggunakan satu user ID dan dapat sekaligus mengakses seluruh rekening yang dimiliki.

d. Sistem Keamanan *Mobile Banking*

Penggunaan *Mobile Banking* sangat berpotensi mengefisiensi biaya sekaligus meningkatkan pendapatan, dengan catatan dari aspek keamanan terjaga dan tidak diragukan oleh pengguna *Mobile Banking*, persyaratan aspek keamanan yang harus diperhatikan pihak bank pada media *Mobile Banking* adalah:⁴⁹

- 1) *Confidentiality*, yang mana memberikan jaminan bahwa data-data tidak disadap oleh pihak-pihak yang tidak berwenang, seperti penyadapan pada nama account dan PIN dari pengguna, penyadapan dapat dilakukan pada sisi terminal (komputer) yang digunakan nasabah atau pada jaringan yang mengantarkan data dari nasabah ke penyedia jasa *Mobile Banking*.
- 2) *Integrity*, dimana data tidak boleh dirubah oleh pihak-pihak yang tidak

⁴⁹ Wahyi Busyro Putri Jamilah, Eko Bagus Cahyo Purnomo, Muhammad Lisman, Rika Septianingsih, *Digital Banking* (Riau: Cv. Dotplus Publisher, 2025).

berwenang.

- 3) *Authentication*, digunakan untuk menyakinkan orang yang mengakses *service* dan juga server (web) yang memberikan *service*, mekanisme yang biasa digunakan adalah:
 - a) Sesuatu yang dimiliki (kartu ATM, *chipcard* atau kartu pembayaran)
 - b) Sesuatu yang diketahui (user ID, *password*, PIN)
 - c) Sesuatu yang menjadi bagian dari pemilik (sidik jari, iris mata)
- 4) *Availability*, difokuskan pada ketersediaan layanan, jika sebuah bank menyediakan layanan *Mobile Banking* pada sewaktu-waktu tidak dapat melayani nasabah dengan baik, maka ada kemungkinan dari nasabah tersebut akan berpindah ke bank yang layanan lebih baik.

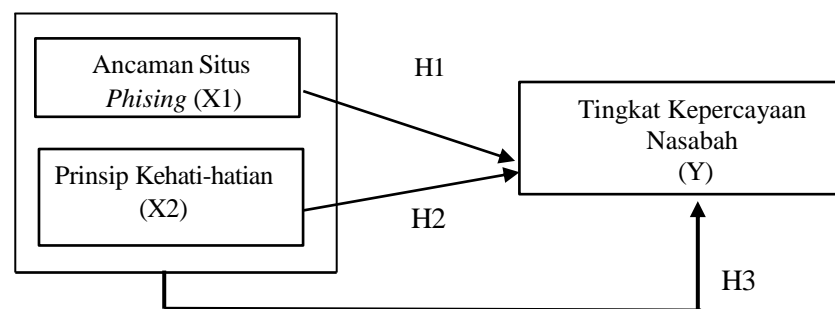
Keamanan menjadi fokus utama dalam penerapan dompet digital sebagai sarana pembayaran. Dengan berbagai lapisan keamanan seperti enkripsi data, otentikasi dua faktor, dan proteksi terhadap aktivitas penipuan, pengguna merasa lebih percaya diri dalam bertransaksi secara daring. Namun, seiring dengan kemajuan teknologi, tantangan keamanan pun semakin kompleks, sehingga perlu adanya kewaspadaan yang terus menerus. Selain keamanan, kemudahan menjadi daya tarik utama dompet digital.

Proses pembayaran yang cepat, mudah, dan efisien memberikan pengalaman yang nyaman bagi konsumen. Dompet digital menyederhanakan transaksi dan memberikan kenyamanan kepada pengguna dengan menghilangkan kebutuhan membawa kartu fisik atau mata uang. Namun, kemudahan ini juga dapat memicu perilaku konsumtif, di mana konsumen cenderung lebih impulsif

dalam pengeluaran mereka karena ketidaknyamanan batasan fisik yang umumnya terdapat pada metode pembayaran tradisional. Selain itu, promosi yang terintegrasi dalam dompet digital memberikan daya tarik tambahan bagi pengguna.

C. Kerangka Pikir

Kerangka pikir adalah sebuah model konseptual pada penelitian tentang bagaimana teori berhubungan dengan berbagai faktor yang telah diidentifikasi sebagai masalah yang penting, dan dijelaskan secara teoritis pertautan antar variabel yang akan diteliti. Adapun kerangka pikir yang digunakan peneliti adalah sebagai berikut:



Gambar 2.1 Kerangka Pikir

Keterangan:

- : Pengaruh Parsial
 → : Pengaruh Simultan

Dalam penelitian ini digunakan model kerangka pikir operasional, dikarenakan untuk mengetahui apakah ada hubungan antara variabel satu dengan yang lain. Di mana pada kerangka pikir tersebut, dapat dijelaskan bahwa bagaimana pengaruh dari masing-masing variabel independent/bebas yaitu

Ancaman situs *Phising* (X1) dan Prinsip Kehati-hatian (X2) terhadap variabel dependen/terikat yaitu Kepercayaan Nasabah (Y). Kemudian dari kedua variabel bebas tersebut apakah secara simultan berpengaruh terhadap variabel terikat (Kepercayaan Nasabah). Dalam penelitian ini fokus terhadap variabel bebas (ancaman situs *Phising* dan prinsip kehati-hatian) dalam mempengaruhi variabel terikat (Kepercayaan Nasabah). Seperti, tingkat adopsi *e-money*, penggunaan *e-money* dalam transaksi ekonomi, serta kesesuaian penggunaan *e-money* dalam prinsip-prinsip ekonomi Islam. Dengan pemilihan variabel-variabel tersebut dalam teori ekonomi Islam, didasarkan kepada beberapa faktor seperti pemahaman yang baik tentang prinsip ekonomi Islam akan mempengaruhi penggunaan tiap individu dalam menggunakan *e-money* yang sesuai dengan nilai-nilai Islam, kemudahan dalam menggunakan layanan *e-money* akan meningkatkan adopsi teknologi tersebut, serta kepercayaan akan memastikan bahwa *e-money* digunakan dengan keyakinan bahwa itu sesuai dengan prinsip-prinsip ekonomi Islam. Kaitannya antara ketiga variabel tersebut adalah pemahaman yang baik akan meningkatkan kepercayaan terhadap penggunaan layanan *e-money*, sementara kemudahan penggunaan akan memfasilitasi penerapan prinsip-prinsip ekonomi Islam dalam menggunakan layanan tersebut.

B. Hipotesis Penelitian

Adapun menurut Sugiyono hipotesis merupakan jawaban sementara terhadap rumusan masalah penelitian serta dikatakan sebagai jawaban sementara karena jawaban yang diberikan hanya berdasarkan teori relevan serta belum berdasarkan

dengan fakta- fakta empiris yang diperoleh melalui pengumpulan data.⁵⁰ Dengan demikian hipotesis dapat dikatakan sebagai jawaban teoritis. Hipotesis dalam penelitian ini adalah sebagai berikut:

1. Ho: Variabel ancaman *Phising* tidak berpengaruh signifikan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*.
H1: Variabel ancaman *Phising* berpengaruh signifikan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*.
2. Ho: Variabel prinsip kehati-hatian tidak berpengaruh signifikan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*.
H2: Variabel prinsip kehati-hatian berpengaruh signifikan terhadap kepercayaan nasabah pengguna *mobile banking*
3. Ho: Variabel ancaman *Phising* dan prinsip kehati-hatian secara simultan tidak berpengaruh signifikan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*.
H3: Variabel ancaman *Phising* dan prinsip kehati-hatian secara simultan berpengaruh signifikan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*.

⁵⁰ Sugiono, *Metode Penelitian Kuantitatif, Kualitatif Dan R&D* (Bandung: Alfabeta, 2021).

BAB III

METODE PENELITIAN

A. Jenis Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian asosiatif (kausal). Pendekatan kuantitatif digunakan karena penelitian ini berfokus pada pengumpulan dan analisis data dalam bentuk angka yang diolah menggunakan teknik statistik untuk menguji hipotesis yang telah dirumuskan.⁵¹ Sementara itu, jenis penelitian asosiatif (kausal) dipilih karena penelitian ini bertujuan untuk mengetahui hubungan sekaligus pengaruh antara variabel independen⁵², yaitu ancaman *phishing* dan prinsip kehati-hatian, terhadap variabel dependen yaitu tingkat kepercayaan nasabah pengguna *mobile banking*.

Penelitian asosiatif digunakan ketika peneliti ingin mengetahui hubungan serta pengaruh antara dua variabel atau lebih. Dalam penelitian ini, peneliti tidak hanya menggambarkan fenomena yang terjadi, tetapi juga menganalisis sejauh mana ancaman *phishing* dan prinsip kehati-hatian memengaruhi tingkat kepercayaan nasabah dalam menggunakan *mobile banking*. Oleh karena itu, penelitian ini dilakukan dengan pengujian hipotesis secara statistik untuk mengetahui kekuatan serta arah hubungan antar variabel.

Penelitian ini melibatkan tiga variabel penelitian, yang terdiri dari variabel independen (X) yaitu ancaman *phishing* (X1) dan prinsip kehati-hatian (X2), serta

⁵¹ Desma Erika Naidin Syamsuddin, Rizky Dewantara, Ida Bagus, *Metode Penelitian Kuantitatif* (Mataram: Sanabil Publishing, 2022).

⁵² Edy Purwanto, *Metodologi Penelitian Kuantitatif* (Yogyakarta: pustaka pelajar, 2023).

variabel dependen (Y) yaitu tingkat kepercayaan nasabah pengguna *mobile banking*. Data penelitian dikumpulkan melalui kuesioner tertutup dengan menggunakan *skala Likert* yang diberikan kepada responden sebagai subjek penelitian. Selanjutnya, data yang diperoleh dianalisis menggunakan analisis regresi linier berganda untuk mengetahui pengaruh masing-masing variabel independen terhadap variabel dependen.

B. Lokasi dan Waktu Penelitian

Penelitian ini dilaksanakan Bank BSI Ratulangi Palopo dan kampus UIN Palopo pada Fakultas Ekonomi dan Bisnis Islam yang berlokasi di Jl. Bitti, Kelurahan Balandai, Kecamatan Bara, Kota Palopo, Sulawesi Selatan. Pemilihan lokasi ini didasarkan pada pertimbangan strategis dan relevansi dengan fokus penelitian, yaitu untuk menganalisis pengaruh ancaman *phishing* dan prinsip kehati-hatian memengaruhi tingkat kepercayaan nasabah dalam menggunakan *mobile banking* dinilai memenuhi kriteria yang sesuai dengan rumusan masalah yang diajukan. Adapun waktu pelaksanaan penelitian berlangsung selama satu bulan, terhitung pada Mei hingga Juni 2025.

C. Defenisi Operasional Variabel

Definisi operasional adalah penjelasan rinci mengenai setiap variabel penelitian berdasarkan indikator yang menyusunnya. Dengan kata lain, spesifikasi variabel-variabel penelitian yang secara konkret terkait dengan realitas yang akan diukur dan diamati oleh peneliti.⁵³

⁵³ Sumardin Satriadi, Anoesyirwan Moeins, *Metodologi Penelitian Kuantitatif* (Sumatra Barat: Cv. Azka Pustaka, 2023).

Tabel 3.1 Tabel Definisi Operasional Variabel

No	Variabel	Definisi Operasional	Indikator
1.	Ancaman Situs Phising (X1)	<i>Phishing</i> merupakan ancaman yang menggunakan teknik rekayasa sosial untuk menyamarkan sebagai entitas resmi dan menipu pengguna, dan menyerang berbagai sektor industri, termasuk perbankan, yang menjadi sasaran nomor 1	1. Pengetahuan 2. Logika ⁵⁴
2.	Prinsip Kehati-hatian (X2)	Prinsip kehati-hatian (<i>prudent banking principle</i>) adalah suatu asas atau prinsip yang menyatakan bahwa bank dalam menjalankan fungsi dan kegiatan usahanya wajib bersikap hati-hati (<i>prudent</i>) dalam rangka melindungi dana masyarakat yang dipercayakan padanya termasuk dalam penyaluran dana yang berasal dari dana yang dihimpun tersebut.	1. Transparansi 2. Responsibility 3. Kewajaran. ⁵⁵
3.	Tingkat Kepercayaan Nasabah (Y)	Kepercayaan konsumen tentang kemungkinan adanya hubungan antara perbankan dengan nasabahnya.	1. Kemampuan. 2. Integritas 3. Kebaikan Hati ⁵⁶

D. Populasi Dan Sampel

1. Populasi

Populasi menunjukkan suatu wilayah generalisasi yang mencakup entitas atau subjek yang memiliki atribut dan sifat tertentu yang ditetapkan oleh peneliti untuk diselidiki, yang kemudian menghasilkan kesimpulan. Ranah konseptual ini tidak hanya berkaitan dengan individu, tetapi juga mencakup entitas dan elemen sifat lainnya. Ruang lingkup populasi lebih dari sekadar representasi numerik dari subjek atau objek yang diteliti, tetapi juga merangkum seluruh atribut dan sifat

⁵⁴ Efy Zam, *Phising: Cara Mudah Menyadap Password & Pencegahannya* (Jakarta Selatan: MediaKita, 2023).

⁵⁵ Bambang Rianto Rustam, *Manajemen Risiko Perbankan Syariah Di Indonesia* (Jakarta: Penerbit Salemba, 2024).

⁵⁶ Rahmadani Hidayat, Sarjon Defit, And Wardana, *Membangun Loyalitas Pelanggan Melalui Kepercayaan: Perspektif Manajemen Pemasaran* (Bali: Cv. Intelektual Manifes Media, 2025).

yang melekat pada subjek atau objek tersebut.⁵⁷

Dalam penelitian ini yang menjadi populasi adalah seluruh mahasiswa Fakultas Ekonomi dan Bisnis Islam UIN Palopo tahun 2025 yang berjumlah 2575 mahasiswa. (sumber website FEBI UIN Palopo, tahun ganjil 2025).

2. Sampel

Sampel merupakan bagian dari jumlah dan atribut yang ditemukan dalam populasi yang lebih besar. Dalam kasus- kasus di mana populasi sangat luas dan mempelajari setiap elemen tidak memungkinkan karena keterbatasan sumber daya keuangan, waktu, dan tenaga, peneliti dapat memilih untuk memeriksa sebagian dari populasi tersebut, yang dikenal sebagai sampel.⁵⁸ Wawasan yang diperoleh dari menganalisis sampel diekstrapolasi untuk membuat kesimpulan tentang seluruh populasi. Misalnya peneliti memiliki keterbatasan waktu penelitian, dana penelitian terbatas, tenaga peneliti terbatas maka peneliti mengambil sampel. Karakteristik sampel akan digunakan untuk penarikan kesimpulan secara general terhadap populasi.

Pengambilan sampel yang digunakan pada penelitian ini adalah menggunakan metode *criterion. sampling* dengan Teknik *purposive* atau *judgmental sampling*. Proses penentuan sampel dilakukan dengan memilih responden yang memenuhi kriteria tertentu yang relevan dengan tujuan penelitian. Alasan peneliti menggunakan metode tersebut dikarenakan peneliti menganggap teknik *criterion* sampling sangat berguna untuk penelitian yang

⁵⁷ Muhammad Aswar Ahmad Ibrahim Andi, Asrul Haq Alang, Madi, Baharuddin and Darmawati, *Metodologi Penelitian*, ed. Ilyas Ismail (jakarta: Guna Darma Ilmu, 2022).

⁵⁸ Sodik And Siyoto, *Dasar Metodologi Penelitian, Dasar Metodologi Penelitian* (Yogyakarta: Media Publishing, 2023).

mempunyai responden dengan pengalaman atau karakteristik spesifik, penggunaan metode ini adalah cara yang akurat untuk memilih sampel dari jumlah populasi yang lebih besar. adapun keunggulan dari metode sampling ini adalah peneliti dapat lebih mudah menentukan anggota sampel dengan relevansi data, hasilnya cepat diperoleh, serta pengumpulan data menjadi lebih efisien karena hanya individu yang memenuhi kriteria yang diikutsertakan, metode ini menghemat waktu dan sumber daya dalam proses pengumpulan data.⁵⁹

Penetapan jumlah sampel yang digunakan pada penelitian ini menggunakan rumus *Slovin* sebagai berikut.⁶⁰

$$n = \frac{N}{1 + N(e)^2}$$

Keterangan:

n : Jumlah Sampel

N : Jumlah Populasi

e : Batas toleransi kesalahan, sebesar 10% atau 0,1.

Dengan perhitungan sampel sebagai berikut:

$$n = \frac{2575}{1 + (2575)(0,1)^2}$$

$$n = \frac{2575}{1 + (2575)(0,01)}$$

$$n = \frac{2575}{1 + (25,76)}$$

$$n = \frac{2575}{26,76}$$

⁵⁹ H Sastrawan and H Menap, *Fundamen Riset Kuantitatif* (Yogyakarta: Deepublish, 2024).

⁶⁰ Azharsyah Ibrahim, *Metodologi Penelitian Ekonomi Dan Bisnis Islam* (Jakarta Timur: Bumi Aksara, 2023).

Berdasarkan perhitungan menggunakan rumus slovin, ukuran sampel minimum adalah 96,71 responden, maka dari itu peneliti membulatkan menjadi 100 responden. Jadi sampel yang digunakan dalam penelitian ini adalah 100 nasabah.

$$n = 96,71$$

E. Teknik Pengumpulan Data

1. Observasi merupakan metode pengumpulan data yang dilakukan dengan cara melakukan pengamatan secara langsung terhadap objek penelitian.⁶¹. Tujuan dari observasi adalah untuk memperoleh informasi yang relevan dengan permasalahan penelitian. Dalam penelitian ini, observasi dilakukan dengan mengamati fenomena penggunaan layanan *mobile banking*, khususnya yang berkaitan dengan ancaman *phishing*, prinsip kehati-hatian nasabah, serta tingkat kepercayaan nasabah dalam menggunakan layanan *mobile banking*. Observasi ini digunakan untuk memperoleh gambaran awal mengenai perilaku dan kewaspadaan nasabah dalam menggunakan layanan perbankan digital.
2. Kepustakaan merupakan teknik pengumpulan data yang dilakukan dengan cara membaca, mempelajari, dan menelaah berbagai sumber literatur yang berkaitan dengan topik penelitian. Sumber tersebut dapat berupa buku, jurnal ilmiah, skripsi, artikel ilmiah, serta sumber lain yang relevan dengan penelitian mengenai ancaman *phishing*, prinsip kehati-hatian, kepercayaan nasabah, dan penggunaan *mobile banking*. Studi kepustakaan ini bertujuan

⁶¹ Jogianto Hartono, *Metode Pengumpulan Dan Teknik Analisis Data* (Yogyakarta: Andi, 2021).

untuk memperoleh landasan teori serta memperkuat analisis dalam penelitian⁶².

3. Angket/kuesioner, yang berisi daftar pernyataan yang diberikan kepada responden. Angket yang digunakan dalam penelitian ini berbentuk angket tertutup, di mana setiap pernyataan sudah dilengkapi dengan pilihan jawaban yang dapat dipilih oleh responden. Skala yang diterapkan dalam angket ini adalah *Skala Likert*, di mana responden diminta mengisi dengan memberi tanda centang pada kolom yang telah disediakan, yang disebarikan melalui *Google Form*. *Skala Likert* merupakan metode untuk mengukur sikap dengan mengungkapkan persetujuan atau ketidaksetujuan terhadap suatu subjek, objek, atau peristiwa tertentu.⁶³ Umumnya, *Skala Likert* menggunakan lima tingkat penilaian, yaitu:⁶⁴

Sangat Setuju (SS) = Diberi Nilai 4

Setuju (S) = Diberi Nilai 3

Tidak Setuju (TS) = Diberi Nilai 2

Sangat Tidak Setuju (STS) = Diberi Nilai 1

F. Instrument Penelitian

Pengolahan data dilakukan dengan menggunakan perangkat lunak *Statistical Product and Service Solutions* (SPSS) versi 26 sebagai alat bantu analisis. Data hasil pengolahan disajikan dalam bentuk tabel dan statistik

⁶² Jogianto Hartono, *Metode Pengumpulan Dan Teknik Analisis Data* (Yogyakarta: Andi, 2021).

⁶³ Jumari Ustiyawati Hardani, Helmina Andriani, *Metode Penelitian Kualitatif & Kuantitatif* (Yogyakarta: Pustaka Ilmu, 2022).

⁶⁴ Indra Prasetia, *Metodologi Penelitian Pendekatan Teori Dan Praktik*, Ed. Emilda Sulasmi Akrim (Medan: Umsu Press, 2022).99

deskriptif. Untuk memastikan kelayakan instrumen penelitian, dilakukan pengujian validitas dan reliabilitas terlebih dahulu. Analisis data menggunakan metode regresi linier berganda, yang kemudian dilanjutkan dengan pengujian hipotesis guna mengetahui sejauh mana pengaruh variabel independen terhadap variabel dependen. Pengujian hipotesis meliputi analisis regresi berganda, koefisien determinasi (R^2), dan uji-t parsial.

G. Uji Validitas dan Reliabilitas Instrumen

Uji validitas digunakan untuk menentukan apakah suatu kuesioner dapat dianggap sah atau tidak. Kuesioner dianggap valid jika pertanyaannya mampu mengungkapkan informasi yang sesuai dengan tujuan pengukurannya. Menurut Sugiono, uji validitas bertujuan untuk memastikan apakah kuesioner tersebut valid atau tidak. Uji validitas dilakukan dengan menghitung korelasi antara setiap pertanyaan dengan skor totalnya. Nilai korelasi yang diperoleh kemudian dibandingkan dengan nilai kritis pada tabel korelasi r . Jika nilai r hitung lebih besar dari r tabel, maka data tersebut dianggap signifikan (valid) dan dapat digunakan dalam pengujian hipotesis. Sebaliknya, jika nilai r hitung lebih kecil dari r tabel, data tersebut dianggap tidak signifikan (tidak valid) dan tidak akan digunakan dalam pengujian hipotesis penelitian.⁶⁵

Uji reliabilitas adalah metode untuk mengevaluasi konsistensi suatu kuesioner yang berfungsi sebagai indikator dari variabel tertentu. Sebuah indikator dianggap reliabel atau andal jika jawaban responden terhadap pertanyaan tetap konsisten atau stabil dari waktu ke waktu. Alat ukur dianggap andal jika

⁶⁵ Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, Dan Tindakan* (Bandung: IKAPI, 2022).

menghasilkan hasil yang stabil, yang diukur melalui koefisien reliabilitas. Keandalan mengacu pada sejauh mana suatu alat mampu mengukur perbedaan individu dengan akurat. Keandalan penting karena data yang tidak andal tidak dapat diolah lebih lanjut.⁶⁶

Uji reliabilitas dalam penelitian ini dilakukan menggunakan rumus *Alpha Cronbach* (α). Sebuah konstruk atau variabel dianggap reliabel jika memiliki nilai *Cronbach Alpha* lebih dari 0,60. Pengukuran reliabilitas instrumen didasarkan pada nilai koefisien *Cronbach Alpha*, di mana semakin mendekati angka 1, semakin tinggi konsistensi dan reliabilitasnya. Menurut Sekaran, tingkat reliabilitas dibagi berdasarkan kriteria nilai alpha sebagai berikut:⁶⁷

0,80 - 1,0 = Reliabilitas Baik

0,60 – 0,79 = Reliabilitas Diterima

<0,60 = Reliabilitas Buruk

H. Teknik Analisis Data

1. Uji Asumsi Klasik

a. Uji Normalitas

Uji normalitas digunakan untuk menentukan apakah populasi data terdistribusi normal atau tidak⁶⁸. Hal ini penting untuk memastikan pemilihan uji statistik yang tepat, karena sebagian besar uji statistik mengharuskan data memiliki distribusi normal. Pengujian dilakukan menggunakan program SPSS

⁶⁶ Yaya Jakaria, *Mengolah Data Penelitian Kuantitatif Dengan SPSS* (Jakarta: Alfabeta, 2024).

⁶⁷ Sekaran, R Bougie, *Research Methods For Business: A Skill Building Approach* (John Wiley & Sons, 2023).

⁶⁸ Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, Dan Tindakan* (Bandung: IKAPI, 2022).

versi 26. Data dianggap berdistribusi normal jika nilai signifikansi lebih besar dari 0,05. Sebaliknya, jika nilai signifikansi lebih kecil dari 0,05, maka data dianggap tidak terdistribusi normal.

b. Uji Multikolinearitas

Pengujian ini bertujuan untuk mengetahui apakah terdapat korelasi antar variabel dalam model regresi linier berganda. Model regresi yang baik seharusnya bebas dari masalah multikolinearitas. Salah satu metode untuk mendeteksi adanya multikolinearitas adalah dengan menganalisis nilai Tolerance dan *Variance Inflation Factor* (VIF)⁶⁹.

c. Uji Heterokedastisitas

Uji heteroskedastisitas dilakukan untuk mendeteksi ada tidaknya pelanggaran terhadap asumsi klasik, yaitu ketidaksamaan varian residual pada setiap tingkat pengamatan dalam model regresi. Salah satu syarat utama yang harus dipenuhi dalam model regresi adalah tidak terjadinya heteroskedastisitas. Untuk mengidentifikasi gejala tersebut, digunakan metode pengujian Glesjer.⁷⁰

2. Uji Hipotesis

a. Regresi Linear Berganda

Data dalam penelitian ini merupakan data kuantitatif yang diperoleh melalui penyebaran kuesioner kepada responden. Analisis data dalam penelitian ini bertujuan untuk mengetahui pengaruh ancaman *phishing* dan prinsip kehati-hatian terhadap tingkat kepercayaan nasabah pengguna *mobile banking*. Oleh karena itu, teknik analisis data yang digunakan adalah analisis regresi linier

⁶⁹ Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, Dan Tindakan* (Bandung: IKAPI, 2022).

⁷⁰ Edi Riadi, *Statistika Penelitian "Analisis Manual Dan Ibm SPSS"* (Yogyakarta: Andi Offset, 2023).

berganda, yaitu suatu metode statistik yang digunakan untuk menganalisis hubungan serta pengaruh antara dua atau lebih variabel independen terhadap satu variabel dependen.

Analisis regresi linier berganda digunakan dalam penelitian ini karena terdapat lebih dari satu variabel bebas yang diduga memengaruhi variabel terikat. Variabel independen dalam penelitian ini terdiri dari ancaman *phishing* (X1) dan prinsip kehati-hatian (X2), sedangkan variabel dependen dalam penelitian ini adalah tingkat kepercayaan nasabah pengguna *mobile banking* (Y). Melalui analisis ini, peneliti dapat mengetahui sejauh mana pengaruh masing-masing variabel independen terhadap variabel dependen, baik secara parsial maupun secara simultan.

Rumus regresi sederhana yang digunakan adalah sebagai berikut:⁷¹

$$Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + \dots + e$$

Keterangan:

Y = Kepercayaan Nasabah

X₁ = Ancaman *Phising*

X₂ = Prinsip Kehati-hatian

A = Konstanta/Kemiringan Slope

β₁ dan β₂ = Koefisien regresi masing-masing variabel

e = *Error Term* (variabel pengganggu) atau residual

Dalam penelitian ini, uji regresi sederhana akan dilakukan menggunakan program SPSS untuk efisiensi waktu.

b. Uji Koefisien Determinasi (R²)

Koefisien determinasi merupakan kuadrat dari koefisien korelasi yang

⁷¹ Priyanto Duwi, *Mandiri Belajar Analisis Data Dengan Spss* (Yogyakarta: Media Kom, 2021)77.

dikalikan dengan 100%. Tujuannya adalah untuk mengetahui sejauh mana variabel X berkontribusi atau mempengaruhi variabel Y. Pengaruh variabel X terhadap variabel Y dapat dilihat pada tabel Model Summary di kolom *R Square*. Nilai tersebut kemudian diubah menjadi bentuk persentase.⁷²

c. Uji Parameter Individual (Uji T)

Uji t digunakan untuk menguji sejauh mana pengaruh variabel independen secara parsial terhadap variabel dependen. Uji ini dilakukan dengan membandingkan nilai t hitung dengan t tabel. Pengaruh variabel X terhadap variabel Y dapat dilihat pada tabel (*Coefficients*) di kolom t (hitung). Jika nilai t (hitung) lebih besar dari t (tabel), maka H_0 ditolak, atau jika nilai signifikansi kurang dari 0,05, maka H_0 juga ditolak.⁷³

d. Uji Signifikansi Simultan (Uji F)

Uji F digunakan untuk mengetahui pengaruh variabel independen secara bersama-sama terhadap variabel dependen. Hubungan yang dianalisis memiliki interpretasi sebagai berikut: apabila nilai F-hitung lebih kecil dari F-tabel, maka H_0 diterima dan H_a ditolak, yang berarti variabel independen secara simultan tidak memiliki pengaruh terhadap variabel dependen. Sebaliknya, jika F-hitung lebih besar dari F-tabel, maka H_0 ditolak dan H_a diterima, yang menunjukkan bahwa variabel independen secara simultan berpengaruh signifikan terhadap variabel dependen.⁷⁴

⁷² Yaya Jakaria, *Mengolah Data Penelitian Kuantitatif Dengan SPSS* (Jakarta: Alfabeta, 2024).

⁷³ Priyanto Duwi, *Mandiri Belajar Analisis Data Dengan Spss* (Yogyakarta: Media Kom, 2021).

⁷⁴ Pandriadi Et Al., *Statistika Dasar* (Bandung: Penerbit Widina, 2023).

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Hasil Penelitian

1. Gambaran Umum Lokasi Penelitian

Lokasi yang menjadi objek pada penelitian ini yaitu Bank Syariah Indonesia (BSI) KCP Palopo Ratulangi. Jl. Ratulangi No. 62 A-B, Kota Palopo, Sulawesi Selatan

a. sejarah Bank Syariah Indonesia (BSI)



Gambar 4.1 Logo Bank Syariah Indonesia (BSI)

Pada tahun 2010 merupakan tahun di dirikannya bank syariah, yang kemudian di dasarkan pada prinsip syariah dengan tujuan memberi informasi kepada masyarakat untuk mengembangkan bank syariah dengan tujuan untuk memajukan pertumbuhan ekonomi islam, dalam berinteraksi dan mengembangkan usaha usaha lainnya yang berkaitan dengan prinsip islam namun di balik di dirikannya bank syariah, pihak pihak bank sudah melakukan evaluasi di kota palopo dalam pengembangan bank syariah, setelah melakukan observasi pihak bank mendiskusikan apakah tempat pembangunan bank syariah layak untuk pembangunan, setelah di lakukan uji kelayakan dan hasilnya positif maka keputusannya kota palopo layak membangun bank syariah mandiri cabang

ratulangi cabang palopo. Dan adapun prinsipnya yaitu:

- 1) Tidak menggunakan sistem bunga dalam transaksinya karena bunga merupakan riba
- 2) Melaksanakan perdagangan bisnis sesuai dengan prinsip islam dengan hasil uang yang halal
- 3) Beri zakat sebagaimana kewajiban bagi umat islam yang mampu untuk menyisihkan sebagian hartanya dan diberikan kepada golongan yang berhak menerimannya.

Beberapa tahun terakhir bank syariah mengalami peningkatan dalam produk dan layanan yang berbasis syariah. Hal ini yang membuat pemerintah menggabungkan tiga bank syariah yaitu bank BNI Syariah, BRI Syariah, dan bank Mandiri Syariah yang beralih nama menjadi bank syariah indonesia.

Tanggal 1 februaruari 2021 di resmikannya bank syariah indonesia yang di resmikan oleh bapak presiden joko widodo yang menyatakan bahwa pihak pemerintah dalam hal ini memantau pengembangan pelayanan yang di dasarkan pada prinsip islam yang bertahan di kondisi saat ini tengah menggelak, melalui BSI pemerintah dapat memantau perekonomian saat ini yang di harapkan dapat memberikan dorongan dalam perkembangan pereknomian.

Dengan adanya penggabungan dari tiga bank tersebut di harapkan dapat menjadi identitas baru bagi perbankan syariah yang universal atau moderen serta dapat memberi manfaat bagi masyarakat maupun dunia.

b. Visi dan Misi BSI KCP Cabang Ratulangi Kota Palopo

1) Visi

Visi merupakan sesuatu yang kita ataupun semua pihak dalam organisasi harapkan di masa depan. Dan adapun visi yang di miliki oleh BSI KCP ratulangi kota palopo adalah yaitu menjadi bank yang dapat mendominasi di bidang industri perbankan, miniature UKM, bisnis dan area perusahaan dan menjadi bank syariah yang memiliki inovasi dalam penyimpanan uang serta admimistrasi yang terunggul bagi klien.

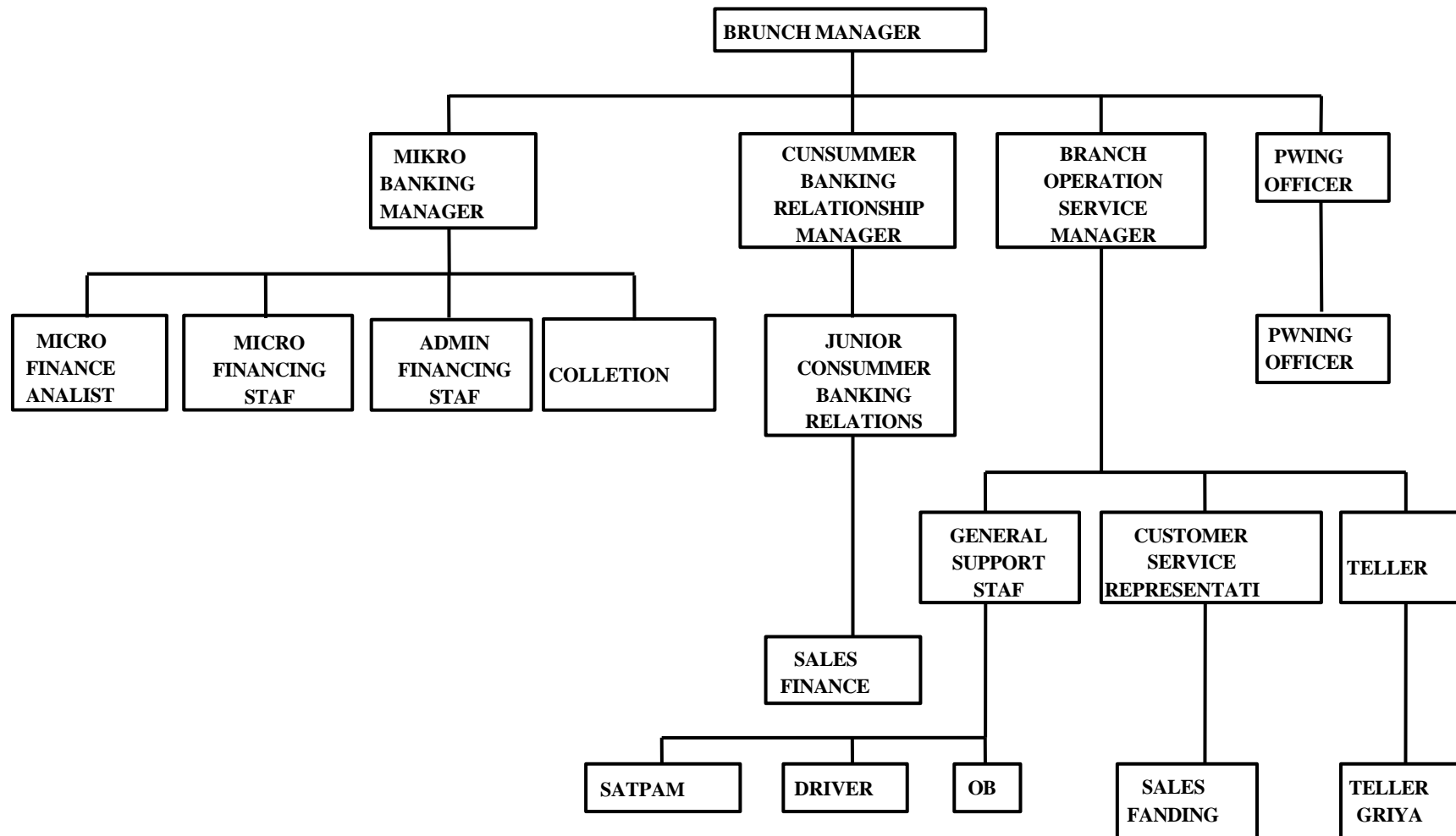
2) Misi

Misi merupakan sebuah pernyataan yang di pergunakan untuk mengetahui tujuan dari sebuah organisasi. Misi BSI KCP Ratulangi palopo yaitu:

- a) Memberi perhatian terhadap masyarakat dan daerah
- b) Melakukan penambahan di industri yang berkaitan dengan profit
- c) Meningkatkan usaha ke tingkat universal
- d) Mengakui manfaat dan perkembangan yang di dapat dari normal bisnis
- e) Menyalurkan pembiayaan kepada segmen ritel dan meningkatkan penghimpun dana murah
- f) Mengembangkan nilai layanan berbasis teknologi sesuai keinginan nasabah
- g) Mengembangkan nilai layanan atau barang berlandaskan teknologi

c. Struktur Organisasi BSI KCP Ratulangi Palopo

Struktur organisasi merupakan suatu sistem yang di pergunakan untuk mendefinisikan setiap pekerjaan dibagi atau di kelompokkan secara teratur.



Gambar 4.2 Struktur Organisasi BSI KCP Ratulangi Palopo

d. Tugas dan Tanggungjawab masing-masing pada BSI KCP Ratulangi Palopo

1) Kepala Cabang:

a) Memimpin dan mengawasi seluruh kegiatan operasional KCP.

- Mengambil keputusan strategis terkait pertumbuhan dan perkembangan KCP.
- Memastikan kepatuhan terhadap peraturan perundang undangan yang berlaku.
- Merekrut dan mengelola sumber daya manusia di KCP.

2) Manajer Mikro *Banking*:

- Mengelola portofolio nasabah mikro.
- Melakukan penjualan produk dan layanan mikro banking.
- Memastikan kualitas layanan dan kepuasan nasabah mikro.
- Melakukan analisis dan evaluasi kinerja portofolio mikro.

3) Teller:

- Melayani transaksi nasabah seperti penyetoran, penarikan, transfer, dan lainnya.
- Memastikan keamanan dan keakuratan transaksi.
- Memberikan informasi terkait produk dan layanan BSI.
- Memberikan pelayanan yang ramah dan profesional.

4) *Customer Service*:

- Melayani pertanyaan dan keluhan nasabah.
- Memberikan informasi terkait produk dan layanan BSI.

- Membantu nasabah dalam proses pembukaan rekening dan penggunaan produk dan menjaga citra positif BSI.

5) *Officer*:

- Melakukan analisis kredit dan pengelolaan risiko.
- Memastikan kepatuhan terhadap prosedur dan kebijakan kredit.
- Mengawasi kualitas portofolio kredit.
- Memberikan rekomendasi terkait persetujuan kredit.

6) Bagian Keuangan:

- Melakukan pencatatan keuangan, termasuk pembukuan dan laporan keuangan.
- Memastikan keakuratan dan kecocokan data keuangan.
- Melakukan analisis keuangan.
- Memproses pembayaran dan penerimaan.

Selain tugas di atas, setiap karyawan juga memiliki tanggung jawab untuk:

- Mematuhi kode etik dan peraturan internal BSI.
- Melaksanakan tugas dengan baik, efisien, dan bertanggung jawab.
- Berkomunikasi dengan baik dengan rekan kerja dan nasabah.
- Berkontribusi pada pencapaian target kinerja KCP.
- Melakukan pengembangan diri dan peningkatan kompetensi

2. Penyajian Data

Berdasarkan penjelasan pada bab sebelumnya, metode yang digunakan dalam pengumpulan data dan informasi yang diperlukan untuk penelitian ini adalah dengan menyebarkan kuesioner atau angket kepada responden. Metode

pengambilan sampel yang digunakan adalah *non-probability sampling* dengan teknik *Purposive Sampling*, di mana responden dipilih berdasarkan kriteria tertentu. Kriteria sampel yang dipilih adalah mahasiswa Fakultas Ekonomi dan Bisnis Islam yang membuka rekening antara bulan Januari 2024 dan juni 2025, dengan total jumlah nasabah sebanyak 2.575 orang. Jumlah responden yang diambil sebanyak 100 orang. Berikut adalah gambaran hasil analisis deskriptif mengenai responden sebagai objek penelitian:

a. Uji Deskriptif Berdasarkan Jenis Kelamin

Pada hasil penelitian didapat gambaran mengenai jenis kelamin responden yang dapat dilihat pada tabel di bawah ini:

Tabel 4.1 Jenis Kelamin Responden

Jenis Kelamin	Jumlah	Persentase (%)
Laki-laki	28	28,0%
perempuan	72	72,0%
Total	100	100%

Sumber: *Output Google Form, data diolah 2025*

Berdasarkan tabel data hasil responden diatas, gender nasabah BSI KCP Ratulangi Palopo menunjukkan nasabah laki-laki sejumlah 28% atau 28 responden. Sedangkan untuk perempuan sejumlah 72% atau 72 responden. Sehingga dapat disimpulkan bahwa nasabah dengan jenis kelamin perempuan lebih banyak dari pada nasabah dengan jenis kelamin laki-laki.

b. Uji Deskriptif Berdasarkan Usia

Melihat kriteria responden pada penelitian ini yaitu nasabah BSI Ratulangi Palopo pengguna layanan digital bank dengan usia 20-25 tahun yang termasuk kedalam pengguna nasabah Bank BSI, maka di dapatkan hasil pada uji deskriptif

berdasarkan usia dapat dilihat sebagaimana berikut:

Tabel 4.2 Usia Responden

Usia	Jumlah	Persentase (%)
<20 tahun	20	20%
20-25 tahun	80	80%
Total	100	100%

Sumber: *Output Google Form, data diolah 2025*

Tabel diatas menunjukkan bahwa usia responden lebih dominan di usia <20 tahun dan 20-25 tahun, dengan presentase usia <20 tahun sebanyak 20 orang atau 20%. Sedangkan usia responden dari 20-25 tahun sebanyak 80 orang atau 80%. Sehingga dapat dilihat bahwa responden mahasiswa nasabah BSI kebanyakan adalah usia 20- tahun dengan jumlah 80 orang dari 100 responden.

3. Analisis dan Pengujian Hipotesis

Variabel dalam penelitian ini terdiri atas variabel bebas (independen), yaitu ancaman *phishing* sebagai variabel X1 dan prinsip kehati-hatian sebagai variabel X2, serta variabel terikat (dependen), yaitu tingkat kepercayaan nasabah pengguna *mobile banking* sebagai variabel Y. Data penelitian diperoleh melalui penyebaran kuesioner kepada 100 responden. Untuk menguji validitas dan reliabilitas instrumen penelitian, digunakan bantuan program SPSS versi 26.0.

Berikut disajikan hasil analisis data responden dalam penelitian ini:

a. Uji Instrumen Penelitian

1) Uji Validitas

Uji validitas bertujuan untuk mengetahui apakah suatu kuesioner layak digunakan dalam penelitian. Pengujian ini dilakukan dengan membandingkan nilai r hitung (korelasi Pearson) dengan r tabel. Dalam penelitian ini, nilai N adalah 100, dengan tingkat signifikansi uji dua arah sebesar 0,05 atau 5%.

Degree of freedom (df) dihitung sebagai $N-2$, sehingga $df = 100-2 = 98$. Dengan demikian, r tabel adalah 0,195. Oleh karena itu, setiap butir pertanyaan pada setiap variabel dianggap valid jika memiliki nilai r hitung $>$ r tabel.

Adapun hasil lengkap dari uji validitas disajikan sebagai berikut:

Tabel 4.3 Hasil Uji Validitas

Variabel	Item	R Hitung	R Tabel	Keterangan
Ancaman <i>Phishing</i>	X1.1	0.842	0.195	Valid
	X1.2	0.893	0.195	Valid
	X1.3	0.850	0.195	Valid
	X1.4	0.854	0.195	Valid
Prinsip Kehati- Hatian	X2.1	0.550	0.195	Valid
	X2.2	0.918	0.195	Valid
	X2.3	0.920	0.195	Valid
	X2.4	0.909	0.195	Valid
Tingkat Kepercayaan Nasabah	Y1	0.904	0.195	Valid
	Y2	0.899	0.195	Valid
	Y3	0.866	0.195	Valid
	Y4	0.901	0.195	Valid

Sumber: hasil olah SPSS 2025

Merujuk pada Tabel 4.3, seluruh item pernyataan dalam instrumen untuk variabel X1, X2 dan Y terbukti valid. Validitas ini ditunjukkan melalui perbandingan antara nilai r hitung dan r tabel, di mana nilai r hitung pada masing-masing item lebih tinggi dari nilai r tabel, sehingga dapat disimpulkan bahwa instrumen tersebut layak digunakan dalam penelitian.

2) Uji Reliabilitas

Uji reliabilitas berkaitan dengan tingkat keandalan dan konsistensi suatu indikator dalam mengukur variabel. Reliabilitas mencerminkan seberapa dapat dipercayanya suatu instrumen pengukuran. Suatu variabel dianggap reliabel apabila nilai *Cronbach's Alpha* melebihi angka 0,60. Adapun hasil pengujian reliabilitas disajikan sebagai berikut:

Tabel 4.4 Hasil Uji Reliabilitas

Variabel	<i>Cronbach's Alpha</i>	Keterangan
Ancaman <i>Phishing</i>	0.882	Reliabel
Prinsip Kehati-Hatian	0.842	Reliabel
Tingkat Kepercayaan Nasabah	0.915	Reliabel

Sumber: hasil olah SPSS 2025

Sebagaimana ditunjukkan dalam tabel uji reliabilitas, nilai koefisien *Cronbach's Alpha* untuk ketiga variabel masing-masing berada $>0,60$. Artinya, instrumen yang digunakan dalam penelitian ini memenuhi kriteria reliabilitas yang dapat diterima.

b. Uji Asumsi Klasik

1) Uji Normalitas

Pengujian normalitas dilakukan untuk mengetahui apakah data memiliki distribusi normal atau tidak. Dalam penelitian ini, pengujian normalitas data menggunakan metode *Kolmogorov-Smirnov Test*. Data dianggap berdistribusi normal jika nilai signifikansi dari hasil uji *Kolmogorov-Smirnov* $>0,05$. Hasil pengujian tersebut dapat dilihat pada tabel berikut:

Tabel 4.5. Hasil Uji Normalitas
One-Sample Kolmogorov-Smirnov Test
 Unstandardized
 Residual

N		100
Normal Parameters ^{a,b}	Mean	.0000000
	Std. Deviation	1.35135473
	Absolute	.189
Most Extreme Differences	Positive	.137
	Negative	-.189
Test Statistic		1.189
Asymp. Sig. (2-tailed)		.077 ^c

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

Sumber: hasil olah SPSS 2025

Berdasarkan *output One Sample Kolmogorov-Smirnov* pada Tabel 4.5, diperoleh nilai signifikansi (Asymp Sig. (2-tailed)) sebesar 0,077. Karena nilai tersebut lebih besar dari 0,05 ($0,077 > 0,05$), maka dapat disimpulkan bahwa data variabel penelitian berdistribusi normal. Dengan demikian, data tersebut telah memenuhi salah satu kriteria dalam uji asumsi klasik.

2) Uji Multikolinearitas

Untuk mengidentifikasi apakah terdapat gejala multikolinearitas dalam model regresi yang digunakan, peneliti merujuk pada nilai VIF (*Variance Inflation Factor*) dan *Tolerance* (TOL). Suatu model dikatakan bebas dari multikolinearitas jika nilai VIF berada $<10,00$ dan nilai TOL $>0,10$. Rincian hasil pengujian multikolinearitas tersebut dapat dilihat pada Tabel 4.6 berikut ini:

Tabel 4.6 Hasil Uji Multikolinearitas

Coefficients ^a		Collinearity Statistics	
		Tolerance	VIF
Model 1	Ancaman_Phising_X1	.520	1.922
	Prinsip_Kehati_Hatian_X2	.520	1.922

a. Dependent Variable: tingkat_Kepercayaan_Y
 Sumber: hasil olah SPSS 2025

Hasil pengujian menunjukkan bahwa nilai *Tolerance* pada variabel Ancaman *Phising* (X1) sebesar 0.520 ($0.520 > 0.10$), Prinsip Kehati-hatian (X2) sebesar 0.520 ($0.520 > 0.10$), serta nilai VIF pada variabel Ancaman *Phising* (X1) sebesar 1.922, Prinsip Kehati-hatian (X2) sebesar 1.922 masih berada di bawah batas 10,00. Oleh karena itu, dapat disimpulkan bahwa variabel bebas dalam penelitian ini tidak mengalami masalah multikolinearitas dan telah memenuhi salah satu syarat dalam uji asumsi klasik.

3) Uji Heterokedastisitas

Untuk mengetahui ada atau tidaknya gejala kesamaan atau ketidaksamaan varians residual dalam model regresi yang digunakan, dilakukan pengujian heteroskedastisitas. Suatu model regresi dianggap layak apabila bebas dari permasalahan heteroskedastisitas. Dalam penelitian ini, pengujian heteroskedastisitas dilakukan dengan menggunakan uji glejser. Model regresi dinyatakan tidak mengandung heteroskedastisitas apabila nilai signifikansi berada di atas tingkat kepercayaan 5% atau $> 0,05$, dan sebaliknya apabila di bawah nilai tersebut.

Tabel 4.7 Uji Heteroskedastisitas

Model	Coefficients ^a		Standardized Coefficients Beta	t	Sig.
	Unstandardized Coefficients B	Std. Error			
1 (Constant)	1.485	.949		1.564	.121
Ancaman_Phising_X1	-.111	.067	-.229	-1.648	.103
Prinsip_Kehati_Hatian_X2	.079	.068	.163	1.173	.244

a. Dependent Variable: abs_res

Sumber: hasil olah SPSS 2025

Berdasarkan hasil uji heteroskedastisitas yang ditampilkan pada tabel di atas, diketahui bahwa nilai signifikansi untuk variabel Ancaman *Phising* (X1) adalah 0,103, untuk variabel Prinsip Kehati-hatian (X2) yaitu 0,244. Karena kedua nilai tersebut lebih besar dari 0,05, maka dapat disimpulkan bahwa tidak terdapat gejala heteroskedastisitas pada kedua variabel tersebut. Hal ini menunjukkan bahwa masing-masing variabel memenuhi asumsi klasik terkait dengan kestabilan varians residual.

c. Uji Regresi Linear Berganda

Analisis regresi linear berganda digunakan untuk mengetahui sejauh mana pengaruh variabel layanan, kenyamanan tempat, dan kualitas produk terhadap keputusan pembelian. Selain itu, analisis ini juga bertujuan untuk mengukur seberapa besar kontribusi variabel bebas (independen) dalam memengaruhi variabel terikat (dependen).

Tabel 4.8 Hasil Uji Regresi Linear Berganda

Model	Coefficients ^a		Standardized Coefficients Beta	t	Sig.
	Unstandardized Coefficients B	Std. Error			
1 (Constant)	.700	1.325		.528	.599
Ancaman_Phising_X1	.254	.094	.228	2.711	.008
Prinsip_Kehati_Hatian_X2	.700	.094	.626	7.422	.000

A. Dependent Variable: Tingkat_Kepercayaan_Y

Sumber: hasil olah SPSS 2025

Berdasarkan hasil pada tabel di atas, maka persamaan regresi linear berganda yang diperoleh dapat dituliskan sebagai berikut:

$$\text{Tingkat Kepercayaan nasabah (Y)} = \alpha + \beta_1 X_1 + \beta_2 X_2 + e$$

$$Y = 0.700 + 0,254 X_1 + 0,700 X_2 + e$$

Dimana:

Y = Tingkat Kepercayaan nasabah

α = *constant*

X1 = Ancaman *Phising*

X2 = Prinsip Kehati-hatian

1. Konstanta sebesar 0.700 nilai konstanta mengatakan bahwa pada saat ketiga variabel tersebut dalam keadaan tetap (*constant*), maka jumlah Tingkat Kepercayaan Nasabah (Y) adalah sebesar 0.700.
2. Koefisien regresi X1 (Ancaman *Phising*) dari perhitungan linier berganda dapat dilihat sebesar 0,254. Hal ini berarti setiap ada peningkatan kualitas pada Ancaman *Phising* maka kepercayaan nasabah akan meningkat sebesar 0,254. Ancaman *Phising* dan kepercayaan nasabah terjadi hubungan positif. Jika Ancaman *Phising* mengalami kenaikan maka kepercayaan nasabah juga akan mengalami kenaikan atau bertambah.

3. Koefisien regresi berganda X2 (Prinsip Kehati-hatian) dari perhitungan regresi linier berganda dapat dilihat sebesar 0,700 hal ini berarti setiap ada peningkatan kualitas pada tingkat kehati-hatian maka kepercayaan nasabah akan meningkat sebesar 0,700. Maka Tingkat Kehati-hatian berpengaruh positif terhadap tingkat kepercayaan nasabah. Sehingga apabila tingkat kepercayaan nasabah mengalami kenaikan maka pengguna *Mobile Banking* juga akan bertambah.

d. Uji Hipotesis

1) Uji Parsial (Uji T)

Pengujian t digunakan secara khusus untuk mengevaluasi signifikansi koefisien regresi (*slope*) dari masing-masing variabel independen. Artinya, uji ini bertujuan untuk mengetahui apakah setiap variabel bebas secara individual memiliki pengaruh yang signifikan terhadap variabel dependen. Kriteria pengambilan keputusan dalam uji ini adalah jika nilai signifikansi (*p-value*) < 0,05, maka H_0 ditolak, yang berarti koefisien regresi signifikan secara statistik. Namun, jika nilai signifikansi >0,05, maka H_0 diterima, yang menunjukkan bahwa koefisien regresi tidak signifikan.

Tabel 4.9 Hasil Uji T

Model	Coefficients ^a		Standardized Coefficients	t	Sig.
	Unstandardized Coefficients	Std. Error			
1 (Constant)	.700	1.325		.528	.599
Ancaman_Phising_X1	.254	.094	.228	2.711	.008
Prinsip_Kehati_Hatian_X2	.700	.094	.626	7.422	.000

A. Dependent Variable: Tingkat_Kepercayaan_Y

Sumber: hasil olah SPSS 2025

Berdasarkan hasil analisis regresi parsial (uji t), diketahui bahwa seluruh variabel independen berpengaruh secara signifikan terhadap tingkat kepercayaan nasabah di Bank BSI KCP Ratulangi Palopo. Variabel Ancaman *Phising* (X1) memiliki nilai t hitung sebesar 2.711, yang lebih besar dari t tabel 1.983 ($2.711 > 1.983$), serta nilai signifikansi sebesar $0.008 < 0.05$. Oleh karena itu, hipotesis alternatif (H1) diterima, dan hipotesis nol (H₀) ditolak, yang berarti ancaman *phising* berpengaruh signifikan terhadap tingkat kepercayaan nasabah.

Variabel Prinsip Kehati-hatian (X2) menunjukkan nilai t hitung sebesar 7,422, yang juga lebih besar dari t tabel 1,983 ($7,422 > 1,983$), dengan tingkat signifikansi sebesar $0,000 < 0,05$. Dengan demikian, hipotesis alternatif (H2) diterima dan hipotesis nol (H₀) ditolak. Hal ini menunjukkan bahwa prinsip kehati-hatian memiliki pengaruh yang signifikan terhadap tingkat kepercayaan nasabah.

Selain itu, jika dilihat dari nilai koefisien regresi (B), variabel Prinsip Kehati-hatian (X2) memiliki pengaruh yang lebih besar dibandingkan dengan variabel Ancaman *Phising* (X1), yang ditunjukkan oleh nilai koefisien sebesar 0,700 untuk X2 dan 0,254 untuk X1. Hal ini mengindikasikan bahwa peningkatan penerapan prinsip kehati-hatian oleh pihak bank akan memberikan kontribusi yang lebih dominan dalam meningkatkan tingkat kepercayaan nasabah dibandingkan dengan faktor ancaman *phising*.

2) Uji Simultan (Uji F)

Suatu ketentuan diberlakukan bahwa apabila nilai probabilitas (F hitung) yang ditunjukkan pada kolom signifikansi (sig.) lebih kecil dari tingkat

signifikansi (α) 0,01, maka hipotesis nol (H_0) ditolak. Hal ini menunjukkan bahwa model regresi yang diestimasi dianggap layak digunakan. Sebaliknya, jika nilai probabilitas F hitung lebih besar dari 0,05, maka H_0 diterima, terutama jika F hitung \leq F tabel dan nilai signifikansi melebihi 0,05. Sementara itu, hipotesis ketiga (H_3) diterima apabila variabel pengetahuan dan literasi keuangan secara simultan menghasilkan nilai F hitung yang lebih besar atau sama dengan F tabel dan nilai signifikansinya kurang dari 0,05.

Tabel 4.10 Hasil Uji F ANOVA^a

Model	Sum of Squares	df	Mean Square	F	Sig.
1 Regression	323.450	2	161.725	86.771	.000 ^b
Residual	180.790	97	1.864		
Total	504.240	99			

a. Dependent Variable: Tingkat_Kepercayaan_Y

b. Predictors: (Constant), Prinsip_Kehati_Hatian_X2, Ancaman_Phising_X1
Sumber: hasil olah SPSS 2025

Pada tabel diatas dapat dilihat bahwa hasil pengujian mendapatkan nilai sebesar 81.407. Sehingga dapat di simpulkan bahwa f hitung $86.771 > f$ tabel 2.70 yang berarti nilai f hitung lebih besar dari f tabel maka dinyatakan bahwa variabel ancaman *Phising* (X1) dan prinsip kehati-hatian (X2) secara bersama-sama berpengaruh terhadap tingkat kepercayaan nasabah pengguna *mobile banking*. Hal ini menunjukkan bahwa hipotesis 3 (H_3), Ancaman *Phising* dan Prinsip Kehati-hatian secara simultan berpengaruh terhadap Tingkat Kepercayaan Nasabah pengguna *Mobile Banking*, dapat diterima.

3) Uji Determinasi (Uji R²)

Uji ini digunakan untuk mengetahui berapa besar pengaruh variabel bebas terhadap variabel terikat. Nilai koefisien determinasi yang digunakan yaitu R

Square.

Tabel 4.11 Hasil Uji Koefisien Determinasi

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.801 ^a	.641	.634	1.36522

a. Predictors: (Constant), Prinsip_Kehati_Hatian_X2, Ancaman_Phising_X1

Sumber: hasil olah SPSS 2025

Nilai R Square sebesar 0,641 menunjukkan bahwa variabel Ancaman *Phising* (X1) dan Prinsip Kehati-hatian (X2) secara simultan mampu menjelaskan 64,1% variasi yang terjadi pada variabel tingkat kepercayaan nasabah di Bank BSI KCP Ratulangi Palopo. Artinya, kedua variabel independen tersebut memberikan kontribusi yang cukup kuat dan signifikan dalam memengaruhi tingkat kepercayaan nasabah.

Sementara itu, sisanya yaitu sebesar 35,9% (100% - 64,1%) dijelaskan oleh variabel lain yang tidak dimasukkan dalam model regresi ini, seperti kualitas layanan, keamanan sistem, reputasi bank, maupun faktor psikologis dan pengalaman nasabah. Nilai *R Square* yang berada di atas 0,6 ini mengindikasikan bahwa model regresi memiliki daya jelas yang tergolong baik dalam menjelaskan fenomena kepercayaan nasabah dalam konteks penelitian ini.

Selain itu, nilai Adjusted R Square sebesar 0,634 menunjukkan bahwa setelah disesuaikan dengan jumlah variabel dalam model, kemampuan variabel independen dalam menjelaskan variabel dependen tetap konsisten dan tidak mengalami penurunan yang berarti, sehingga model yang digunakan dapat dikatakan cukup stabil dan layak untuk digunakan dalam analisis lebih lanjut.

B. Pembahasan

1. Pengaruh Variabel Ancaman *Phising* Terhadap Tingkat Kepercayaan Nasabah

Tabel yang diperoleh nilai t hitung sebesar 2,711 yang artinya nilai t hitung $>$ t tabel ($2,711 > 1,983$) dengan signifikansi 0,008 dimana hasil tersebut lebih kecil dari taraf signifikansi sebesar 0,05 atau $0,008 < 0,05$. Maka dapat disimpulkan bahwa secara parsial terdapat pengaruh signifikan antara ancaman *phising* terhadap tingkat kepercayaan nasabah pengguna *mobile banking*.

Hal ini menunjukkan bahwa semakin tinggi persepsi ancaman *phising* yang dirasakan nasabah, maka akan memengaruhi tingkat kepercayaan mereka terhadap layanan *mobile banking*. Ancaman keamanan seperti pencurian data, penipuan, dan kebocoran informasi pribadi menjadi faktor penting yang dapat menurunkan kepercayaan nasabah terhadap sistem perbankan digital.

Temuan ini sejalan dengan teori kepercayaan yang dikemukakan oleh McAllister dalam buku Cherly Kemala, yang menyatakan bahwa kepercayaan terbentuk berdasarkan keyakinan individu terhadap keamanan dan keandalan suatu sistem atau pihak lain.⁷⁵ Dalam konteks ini, apabila nasabah merasa sistem *mobile banking* rentan terhadap serangan *phising*, maka kepercayaan kognitif mereka akan menurun karena adanya keraguan terhadap keamanan sistem tersebut.

Hasil penelitian ini didukung oleh penelitian terdahulu oleh Imelia Damai

⁷⁵ Cherly Kemala Ulfa, *Strategi Meningkatkan Inovasi Kerja* (indra: Penerbit Adab, 2022).

Agustina dkk, yang menyatakan bahwa kejahatan *phising* dalam layanan perbankan digital dapat menurunkan tingkat kepercayaan nasabah karena adanya kekhawatiran terhadap keamanan data pribadi⁷⁶. Selain itu, penelitian oleh Zamzami Akromi Lubis dan Fauzi Arif Lubis juga menunjukkan bahwa persepsi keamanan memiliki pengaruh signifikan terhadap kepercayaan nasabah, khususnya setelah adanya kasus serangan siber pada perbankan.⁷⁷

Dalam perspektif Islam, tindakan *phising* termasuk dalam kategori penipuan (*gharar* dan *tadlis*) yang dilarang. Hal ini sesuai dengan firman Allah SWT dalam QS. Al-Baqarah ayat 188 yang melarang mengambil harta orang lain dengan cara yang batil. Oleh karena itu, adanya ancaman *phising* tidak hanya merugikan secara materi, tetapi juga bertentangan dengan prinsip keadilan dan kejujuran dalam muamalah Islam. Dengan demikian, bank perlu meningkatkan sistem keamanan untuk menjaga kepercayaan nasabah sekaligus menerapkan nilai-nilai syariah.

2. Pengaruh Variabel Prinsip Kehati-hatian Terhadap Tingkat Kepercayaan Nasabah

Tabel yang diperoleh nilai t hitung sebesar 7,422 yang artinya nilai t hitung > t tabel ($7,422 > 1,983$) dengan signifikansi 0,000 dimana hasil tersebut lebih kecil dari taraf signifikansi sebesar 0,05 atau $0,000 < 0,05$. Maka dapat disimpulkan bahwa secara parsial terdapat pengaruh positif dan signifikan antara

⁷⁶ Amai Agusthin Imelia, Christy Nada Dinda, And Ananda Putri Nadia, "Perlindungan Hukum Nasabah Dari Kejahatan Phising Dalam Layanan Perbankan Digital Di Indonesia," *Depositi: Jurnal Publikasi Ilmu Hukum Yuridume.lu: Fakultas Hukum, Universitas Katolik Widya Karya Malang* 2, No. 4 (2024): 132–48.

⁷⁷ Lubis and Lubis, "Pengaruh Persepsi Keamanan Dan Kepercayaan Terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber Di Bank Syariah Indonesia."

prinsip kehati-hatian terhadap tingkat kepercayaan nasabah pengguna *mobile banking*.

Hal ini menunjukkan bahwa semakin baik penerapan prinsip kehati-hatian oleh pihak bank, maka akan semakin meningkatkan tingkat kepercayaan nasabah. Prinsip kehati-hatian yang mencakup aspek transparansi, tanggung jawab, dan keamanan sistem menjadi faktor utama dalam menciptakan rasa aman bagi nasabah dalam menggunakan layanan *mobile banking*.

Temuan ini sejalan dengan teori *prudential banking principle* dalam buku Reza Rian Saputra, yang menyatakan bahwa bank wajib menjalankan kegiatan usahanya secara hati-hati guna melindungi dana masyarakat dan menjaga stabilitas sistem keuangan. Prinsip ini juga berkaitan dengan fungsi bank sebagai *agent of trust*, dimana kepercayaan menjadi fondasi utama dalam hubungan antara bank dan nasabah.⁷⁸

Hasil penelitian ini didukung oleh penelitian terdahulu yang dilakukan oleh Andi Siti Nurbaya Sari, yang menyatakan bahwa prinsip kehati-hatian berpengaruh signifikan dalam mengurangi risiko ancaman *phising* serta meningkatkan keamanan data nasabah.⁷⁹ Selain itu, penelitian oleh Siswanto dan Milda Dwi Lenita juga menegaskan bahwa penerapan prinsip kehati-hatian sangat penting dalam melindungi nasabah dari kejahatan *social engineering fraud*.⁸⁰

⁷⁸ Reza Rian Saputra, *Teori Dasar Manajemen Perbankan Syariah* (Bengkulu: CV Brimedia Global, 2024).

⁷⁹ Andi Siti Nurbaya Sari, "Pengaruh Prinsip Kehati-Hatian Terhadap Ancaman Situs Phising Pada Nasabah Pengguna Internet Banking (Studi Kasus Pada Bank Syariah Di Kota Palopo)" (Palopo: Institut Agama Islam Negeri Palopo, 2021).

⁸⁰ D W I Lenita Milda, "Prinsip Kehati-Hatian Nasabah Perbankan Dalam Menjaga

Dalam perspektif Islam, prinsip kehati-hatian sejalan dengan konsep *tabayyun* sebagaimana dijelaskan dalam QS. Al-Hujurat ayat 6, yang menekankan pentingnya verifikasi informasi sebelum mengambil keputusan. Hal ini menunjukkan bahwa sikap hati-hati dan tidak tergesa-gesa merupakan prinsip penting dalam menjaga keamanan dan kepercayaan dalam aktivitas muamalah. Oleh karena itu, penerapan prinsip kehati-hatian oleh bank tidak hanya penting secara operasional, tetapi juga merupakan bagian dari implementasi nilai-nilai Islam dalam perbankan syariah.

3. Ancaman *Phising* dan Prinsip Kehati-Hatian Terhadap Tingkat Kepercayaan Nasabah Pengguna *Mobile Banking*

Berdasarkan hasil uji simultan (uji F) diperoleh bahwa variabel ancaman *phising* dan prinsip kehati-hatian secara bersama-sama berpengaruh signifikan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*. Hal ini juga diperkuat oleh nilai koefisien determinasi (*R Square*) sebesar 0,641, yang menunjukkan bahwa kedua variabel tersebut mampu menjelaskan 64,1% variasi tingkat kepercayaan nasabah, sedangkan sisanya sebesar 35,9% dipengaruhi oleh variabel lain di luar penelitian ini.

Hal ini menunjukkan bahwa kepercayaan nasabah tidak hanya dipengaruhi oleh satu faktor saja, melainkan kombinasi antara faktor risiko (ancaman *phising*) dan faktor perlindungan (prinsip kehati-hatian). Ketika ancaman meningkat tetapi tidak diimbangi dengan penerapan prinsip kehati-hatian yang baik, maka

kepercayaan nasabah akan menurun. Sebaliknya, jika bank mampu mengelola risiko dengan baik melalui prinsip kehati-hatian, maka kepercayaan nasabah dapat tetap terjaga.

Temuan ini sejalan dengan teori perilaku konsumen dalam layanan digital yang menyatakan bahwa kepercayaan terbentuk dari interaksi antara persepsi risiko dan jaminan keamanan. Semakin tinggi jaminan keamanan yang diberikan, maka semakin tinggi pula kepercayaan pengguna terhadap layanan tersebut.⁸¹

Hasil penelitian ini juga didukung oleh penelitian Zamzami Akromi Lubis dan Fauzi Arif Lubis, yang menunjukkan bahwa persepsi keamanan dan kepercayaan memiliki pengaruh signifikan terhadap loyalitas nasabah.⁸² Hal ini mengindikasikan bahwa keamanan dan kehati-hatian merupakan faktor kunci dalam membangun hubungan jangka panjang dengan nasabah.

Dalam perspektif Islam, kombinasi antara menghindari risiko (*dharar*) dan menerapkan prinsip kehati-hatian merupakan bagian dari konsep masalah (kemaslahatan). Hal ini sejalan dengan QS. An-Nisa ayat 29 yang menegaskan bahwa transaksi harus dilakukan secara adil dan tidak merugikan pihak lain. Dengan demikian, menjaga keamanan sistem dan menerapkan prinsip kehati-hatian bukan hanya strategi bisnis, tetapi juga merupakan tanggung jawab moral dalam menjalankan prinsip ekonomi Islam.

⁸¹ Erwin Et Al., *Ekonomi Manajerial : Teori, Konsep, Strategi \& Aplikasi Komprehensif Ekonomi Manajerial* (Jambi: Pt. Sonpedia Publishing Indonesia, 2023), https://books.google.co.id/books?id=0v_Deaaaqbaj.

⁸² Lubis and Lubis, "Pengaruh Persepsi Keamanan Dan Kepercayaan Terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber Di Bank Syariah Indonesia."

BAB V

PENUTUP

A. Simpulan

Penelitian ini bertujuan untuk menganalisis sejauh mana ancaman *phising* dan prinsip kehati-hatian memengaruhi tingkat kepercayaan nasabah pengguna *mobile banking*. Berdasarkan hasil penelitian, uji hipotesis, dan pembahasan yang telah dilakukan, maka dapat disimpulkan hal-hal berikut:

1. Ancaman *phising* memiliki pengaruh signifikan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*. Temuan ini menunjukkan bahwa dalam konteks layanan perbankan digital, persepsi risiko keamanan seperti pencurian data dan penipuan menjadi faktor penting yang memengaruhi kepercayaan nasabah. Semakin tinggi ancaman yang dirasakan, maka semakin besar potensi penurunan kepercayaan terhadap layanan *mobile banking*. Secara teoritis, hal ini mendukung konsep *perceived risk dan trust*, dimana kepercayaan nasabah sangat dipengaruhi oleh tingkat keamanan sistem yang dirasakan. Secara praktis, hasil ini menuntut pihak perbankan untuk terus meningkatkan sistem keamanan serta edukasi kepada nasabah agar mampu mengidentifikasi dan menghindari ancaman *phising*.
2. Prinsip kehati-hatian memiliki pengaruh signifikan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*. Hal ini menunjukkan bahwa penerapan prinsip kehati-hatian oleh pihak bank, seperti transparansi,

3. tanggung jawab, dan perlindungan data nasabah, mampu meningkatkan rasa aman dan kepercayaan nasabah. Secara teoritis, temuan ini mendukung konsep *prudential banking* dan fungsi bank sebagai *agent of trust*, dimana kepercayaan merupakan fondasi utama dalam hubungan antara bank dan nasabah. Secara praktis, hasil ini mendorong pihak bank untuk secara konsisten menerapkan prinsip kehati-hatian dalam setiap aspek operasional guna menjaga dan meningkatkan kepercayaan nasabah.
4. Ancaman *phising* dan prinsip kehati-hatian secara simultan berpengaruh signifikan terhadap tingkat kepercayaan nasabah pengguna *mobile banking*. Hal ini menunjukkan bahwa kepercayaan nasabah terbentuk dari kombinasi antara persepsi risiko dan jaminan keamanan yang diberikan oleh bank. Dalam perspektif perilaku konsumen digital, kepercayaan merupakan hasil dari pengalaman menyeluruh yang mencakup aspek keamanan sistem dan perlindungan yang diberikan kepada pengguna. Hasil ini mengindikasikan bahwa untuk menjaga kepercayaan nasabah, pihak perbankan tidak hanya perlu meminimalkan risiko ancaman *phising*, tetapi juga harus memperkuat penerapan prinsip kehati-hatian secara berkelanjutan. Oleh karena itu, strategi yang terintegrasi antara peningkatan keamanan teknologi dan penguatan tata kelola perbankan menjadi kunci utama dalam membangun kepercayaan nasabah secara jangka panjang.

B. Saran

Merujuk pada kesimpulan yang telah disampaikan sebelumnya, peneliti

berharap agar penelitian serupa di masa mendatang, khususnya yang berkaitan dengan pengaruh ancaman *phising* dan prinsip kehati-hatian terhadap tingkat kepercayaan nasabah pengguna *mobile banking*, dapat dilakukan dengan lebih baik. Oleh karena itu, peneliti mengajukan beberapa saran kepada pihak-pihak terkait sebagai berikut:

1. Bagi pihak perbankan (khususnya Bank Syariah Indonesia), hasil penelitian menunjukkan bahwa ancaman *phising* dan prinsip kehati-hatian mampu menjelaskan sebesar 64,1% tingkat kepercayaan nasabah. Oleh karena itu, pihak bank disarankan untuk melengkapi faktor-faktor lain yang memengaruhi kepercayaan nasabah, seperti peningkatan kualitas layanan digital, kemudahan penggunaan aplikasi (*user friendly*), serta penguatan sistem keamanan berbasis teknologi terkini. Selain itu, edukasi kepada nasabah mengenai bahaya *phising* dan cara pencegahannya perlu ditingkatkan secara berkelanjutan melalui sosialisasi, notifikasi aplikasi, maupun kampanye digital. Upaya ini diharapkan dapat meningkatkan kepercayaan nasabah secara menyeluruh serta meminimalisir risiko kejahatan siber yang dapat merugikan bank dan nasabah.
2. Bagi mahasiswa, khususnya yang tertarik dalam bidang perbankan syariah dan teknologi keuangan (*fintech*), diharapkan dapat mengembangkan wawasan serta kemampuan analisis dengan melakukan penelitian lanjutan yang berkaitan dengan keamanan digital, perilaku nasabah, dan kepercayaan dalam penggunaan layanan *mobile banking*. Penelitian ini dapat menjadi referensi awal untuk memahami pentingnya aspek keamanan dan kehati-

hatian dalam membangun kepercayaan nasabah di era digital.

3. Bagi peneliti selanjutnya, perlu diperhatikan bahwa penelitian ini hanya mencakup dua variabel utama, yaitu ancaman *phising* dan prinsip kehati-hatian. Oleh karena itu, disarankan agar penelitian selanjutnya dapat menambahkan variabel lain seperti persepsi keamanan, kualitas layanan digital, kemudahan penggunaan, citra merek, maupun kepuasan nasabah. Selain itu, penggunaan metode penelitian yang lebih beragam seperti metode campuran (*mixed-method*) atau pendekatan *longitudinal* dapat memberikan pemahaman yang lebih mendalam mengenai dinamika kepercayaan nasabah dari waktu ke waktu. Dengan demikian, hasil penelitian di masa mendatang diharapkan mampu memberikan kontribusi yang lebih komprehensif bagi pengembangan layanan perbankan digital, khususnya dalam meningkatkan kepercayaan nasabah.

DAFTAR PUSTAKA

- Amarta, Priska Cintya. "Pengaruh Teknologi Digital Dalam Perkembangan Layanan Perbankan Syariah." *Jurnal Ilmiah Research And Development Student (Jis)* 2, No. 3 (2024): 134–45. <https://doi.org/10.59024/jise.v2i3.788>.
- Anugerah Puji Sakti, Endra Syaifuddin Ahmad. "Penerapan Prinsip Kehati-Hatian (Prudential Principle) Dalam Proses Pembiayaan Pada Bank Syariah Di Indonesia (Studi Kasus Bank Syariah Indonesia Kantor Cabang Mataram Nusa Tenggara Barat)." *Jurnal Risalah Kenotariatan* 4, No. 1 (2023). <https://doi.org/10.29303/Risalahkenotariatan.V4i1.96>.
- Ariadi, Fadly, Suhanda Saputra, And Anggreita Tiara Putri. "Sosialisasi Ancaman Dan Pencegahan Phishing Terhadap Pengguna Sosial Media Kepada Siswa / I." *Jari: Jurnal Pengabdian Kepada Masyarakat Republik Indonesia* 1, No. 2 (2023): 10–15. <https://mypublikasi.com/index.php/jari>.
- Astriyanti, Giantari, Rastini, Wardana, And Wardana. *Kepuasan Nasabah Pada Lembaga Keuangan Non Bank*. Bali: Cv. Intelektual Manifes Media, 2023.
- Bank Syariah Indonesia. "Digital Banking Dinilai Optimal, Bsi Raih Penghargaan Best Digital Bank." <https://www.bankbsi.co.id/>. Accessed September 17, 2024. <https://www.bankbsi.co.id/news-update/berita/digital-banking-dinilai-optimal-bsi-raih-penghargaan-best-digital-bank>.
- Budianto, Eka Wahyu. *Determinan Perilaku Nasabah Bank Syariah (2023-2025)*. Malang: Pt. Afanin Media Utama, 2025.
- Chen, Yan, Cheng Yu, Yuan Yuan, Fang Lu, And Wangbing Shen. "The Influence Of Trust On Creativity: A Review." *Frontiers In Psychology* 12 (2021): 706234. <https://doi.org/10.3389/fpsyg.2021.706234>.
- Duwi, Priyanto. *Mandiri Belajar Analisis Data Dengan Spss*. Yogyakarta: Media Kom, 2021.
- Erwin, Rini Setyastuti, Sumantri, Munawar, And Agustina. *Ekonomi Manajerial : Teori, Konsep, Strategi & Aplikasi Komprehensif Ekonomi Manajerial*. Jambi: Pt. Sonpedia Publishing Indonesia, 2023. https://books.google.co.id/books?id=0v_Deaaqbj.
- Fachriah, Pratiwi, Utari, Naturrachma, Ramadhini, Prima, And Nathasia. *Hukum Lembaga Keuangan*. Pekanbaru: Cv. Ekdanta Press, 2025.
- Fadli, Muhammad, Dijan Widijowati, And Dwi Andayani. "Pencurian Data Pribadi Di Dunia Maya (Phising Cybercrime) Yang Ditinjau Dalam Perspektif Kriminologi." *Co-Value Jurnal Ekonomi Koperasi Dan Kewirausahaan* 14, No. 12 (2024).
- Faizal, Muhazzab Alief, Zelyn Faizatul, Binti Nur Asiyah, And Rokhmat Subagyo. "Analisis Risiko Teknologi Informasi Pada Bank Syariah: Identifikasi Ancaman Dan Tantangan Terkini." *Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam* 5, No. 2 (2023): 87–100. <https://doi.org/10.47435/Asy-Syarikah.V5i2.2022>.
- Fery, Febriansyah. *Cybercrime : Kejahatan Di Balik Layar Digital*. Ponorogo: Najaha, 2025.
- Hadzami, Mohammad Rafi. *Inovasi Dan Strategi Keuangan*. Yogyakarta:

- Deepublish, 2025.
- Hardani, Helmina Andriani, Jumari Ustyawati. *Metode Penelitian Kualitatif & Kuantitatif*. Yogyakarta: Pustaka Ilmu, 2020.
- Hartono, Jogianto. *Metode Pengumpulan Dan Teknik Analisis Data*. Yogyakarta: Andi, 2021.
- Hasche, Nina, Linda Höglund, Maria Mårtensson, And Nina Hasche. “Intra-Organizational Trust In Public Organizations – The Study Of Interpersonal Trust In Both Vertical And Horizontal Relationships From A Bidirectional Perspective.” *Public Management Review* 23, No. 12 (2022): 1768–88. <https://doi.org/10.1080/14719037.2020.1764081>.
- Hidayat, Rahmadani, Sarjon Defit, And Wardana. *Membangun Loyalitas Pelanggan Melalui Kepercayaan: Perspektif Manajemen Pemasaran*. Bali: Cv. Intelektual Manifes Media, 2025.
- Ibrahim Andi, Asrul Haq Alang, Madi, Baharuddin, Muhammad Aswar Ahmad, And Darmawati. *Metodologi Penelitian*. Edited By Ilyas Ismail. Jakarta: Guna Darma Ilmu, 2022.
- Ibrahim, Azharsyah. *Metodologi Penelitian Ekonomi Dan Bisnis Islam*. Jakarta Timur: Bumi Aksara, 2023.
- Imelia, Damai Agusthin, Christy Nada Dinda, And Ananda Putri Nadia. “Perlindungan Hukum Nasabah Dari Kejahatan Phising Dalam Layanan Perbankan Digital Di Indonesia.” *Depositi: Jurnal Publikasi Ilmu Hukum Uçpedumelu: Fakultas Hukum, Universitas Katolik Widya Karya Malang* 2, No. 4 (2024): 132–48.
- Indonesia, Badan Perlindungan Konsumen Nasional Republik. “Kasus Phising Makin Marak, Bpknri Bahas Strategi Pencegahan Bareng Pemprov Sulsel.” *Trimbun Makassar*, N.D.
- Indonesia, Dewan Perwakilan Rakyat Republik. “Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan.” *Indonesia*, N.D.
- Iskandar, Octo. “Analisis Kejahatan Online Phishing Pada Masyarakat.” *Leuser: Jurnal Hukum Nusantara* 1, No. 2 (2024): 32–36. <https://journal.myrepublikcorp.com/index.php/leuser/article/view/85>.
- Kemal Idris Balaka, Aulia Rahman Hakim, Frygyta Dwi Sulistyany. “Pencurian Informasi Nasabah Di Sektor Perbankan :” *Yustitiabelen* 10, No. 3 (2024): 105–30. <https://doi.org/https://doi.org/10.36563/Yustitiabelen.V10i2.1167>.
- Lajnah Pentashihan Mushaf Al-Qur’an. *Qur’an Kemenag*. Indonesia, 2022.
- Lestari, Eka. *Layanan Perbankan Fase F*. Medan: Umsu Press, 2024.
- Lestari, Wahyu Bunga. “Pengawasan Dan Perlindungan Ojk Kepada Bsi Terhadap Serangan Cyber Crime Prespektif Uu No.21 Tahun 2011 Serta Maqasis As-Syariah (Studi Kasus Di Ojk Solo).” *Salatiga : Universitas Islam Negeri (Uin) Salatiga*, 2024.
- Lubis, Zamzami Akromi, And Fauzi Arif Lubis. “Pengaruh Persepsi Keamanan Dan Kepercayaan Terhadap Loyalitas Nasabah: Studi Kasus Serangan Siber Di Bank Syariah Indonesia.” *El-Mal: Jurnal Kajian Ekonomi & Bisnis Islam* 5, No. 10 (2024): 4215–30.

- Ma'ruf, Jasman J. *Manajemen Perspektif Indonesia*. Aceh: Usk Press, 2025.
- Maulana, Lutfi, And Nadia Nur Fitriana. "Analisis Dampak Insiden Bsi Error Dan Dugaan Hacking Bank Syariah Indonesia (Bsi) Terhadap Kepercayaan Dan Loyalitas Nasabah Bank Syariah Indonesia Di Kabupaten Subang." *Rayah Al-Islam*, 2024.
- Mcdonough, R. *Cyber Smart: Five Habits To Protect Your Family, Money, And Identity From Cyber Criminals*. Canada: Wiley, 2023.
- Milda, D W I Lenita. "Prinsip Kehati-Hatian Nasabah Perbankan Dalam Menjaga Keamanan Bisnis Dari Social Engineering Fraudud." *Justitiable-Jurnal Hukum Учредители: Universitas Bojonegoro* 7, No. 1 (2024): 82–100.
- Naidin Syamsuddin, Rizky Dewantara, Ida Bagus, Desma Erika. *Metode Penelitian Kuantitatif*. Mataram: Sanabil Publishing, 2022.
- Nisa, Lazarusli, Pribadi, Marzuki, Lisangan. *Keamanan Siber (Cyber Security)*. Padang: Cv. Gita Lentera, 2025.
- Novia Galuh Rima Dona, Rafida, Lidya Angreini. "Pelaksanaan Prinsip Kehati-Hatian Dalam Indonesia Kc Jambi Gatot Subroto." *Jurnal Ekonomica Sharia : Jurnal Pemikiran Dan Pengembangan Ekonomi Syariah* 8 (2023): 205–20. <https://doi.org/10.36908/EsHa.V8i2.589>.
- Pandriadi, P, V N Van Harling, A Wahab, S Vaulina, E K Ningsih, B D H Setyono, V Rizqi, M I Harisuddin, S Gaffar, And Others. *Statistika Dasar*. Bandung: Penerbit Widina, 2023.
- Prasetya, Indra. *Metodologi Penelitian Pendekatan Teori Dan Praktik*. Edited By Emilda Sulasmi Akrim. Medan: Umsu Press, 2022.
- Purwanto, Djoko. *Komunikasi Bisnis*. 3rd Ed. Jakarta: Erlangga, 2022.
- Purwanto, Edy. *Metodologi Penelitian Kuantitatif*. Yogyakarta: Pustaka Pelajar, 2022.
- Putri Jamilah, Eko Bagus Cahyo Purnomo, Muhammad Lisman, Rika Septianingsih, Wahyi Busyro. *Digital Banking*. Riau: Cv. Dotplus Publisher, 2025.
- Rahayuningsih, Titien. *Bank Dan Lembaga Keuangan Lainnya*. Sukoharjo: Epigraf Komunikata Prima, 2024.
- Rahmayati. *Sistem Informasi Manajemen Dan Keamanan Di Lembaga Keuangan Syariah*. Medan: Umsu Press, 2025.
- Riadi, Edi. *Statistika Penelitian (Analisis Manual Dan Ibm Spss)*. Yogyakarta: Andi Offset, 2023.
- Rustam, Bambang Rianto. *Manajemen Risiko Perbankan Syariah Di Indonesia*. Jakarta: Penerbit Salemba, 2024.
- Sahwa Aulia S, Antong, Halim Usman. "Pengaruh Kesadaran Sosial Dan Prinsip-Prinsip Terhadap Kepercayaan Nasabah Di Bank Syariah." *Journal Of Economics, Business And Accounting* 7, No. 6 (2024).
- Santoso, Edy. *Hukum Siber: Permasalahan Hukum Bisnis Di Bidang Teknologi Informasi Dan Komunikasi*. Jakarta: Prenada Media, 2023.
- Saputra, Reza Rian. *Teori Dasar Manajemen Perbankan Syariah*. Bengkulu: Cv Brimedia Global, 2024.
- Sari, Andi Siti Nurbaya. "Pengaruh Prinsip Kehati-Hatian Terhadap Ancaman Situs Phising Pada Nasabah Pengguna Internet Banking (Studi Kasus Pada

- Bank Syariah Di Kota Palopo).” Institut Agama Islam Negeri Palopo, 2021.
- Sastrawan, H, And H Menap. *Fundamen Riset Kuantitatif*. Yogyakarta: Deepublish, 2024.
- Satriadi, Anoesyirwan Moeins, Sumardin. *Metodologi Penelitian Kuantitatif*. Sumatra Barat: Cv. Azka Pustaka, 2023.
- Sekaran, U, And R Bougie. *Research Methods For Business: A Skill Building Approach*. John Wiley & Sons, 2016.
- Sodik, And Siyoto. *Dasar Metodologi Penelitian*. Dasar Metodologi Penelitian. Yogyakarta: Media Publishing, 2015.
- Sugiono. *Metode Penelitian Kuantitatif, Kualitatif Dan R&D*. Bandung: Alfabeta, 2021.
- Ulfa, Cherly Kemala. *Strategi Meningkatkan Inovasi Kerja*. Indra: Penerbit Adab, 2022.
- Vania Trisnawati, Edy Soesanto, Sandra Mutiara Tirta. “Kesadaran Korban Cyber Crime Dalam Kasus Phising.” *Jurnal Ilmu Pendidikan* 1, No. 10 (2025). <https://jutepe-joln.net/index.php/jurperu/article/view/500>.
- Yaya Jakaria. *Mengolah Data Penelitian Kuantitatif Dengan Spss*. Jakarta: Alfabeta, 2024.
- Yoyo Sudaryo, Ferry Kosadi, Mochammad Mukti Ali. *Sistem Informasi Manajemen Berbasis Artificial Intelligence Dan E-Business System*. Yogyakarta: Penerbit Andi, 2024.
- Yuswanita, Annisa, Guslindawati, Wahyu Nengsri Putri, And Jhon Veri. *Keamanan Informasi: Jenis, Prinsip Dan Implementasi Dalam Era Digital*. Sumatera Barat: Fahmi Karya, 2025.
- Zam, Efy. *Phising: Cara Mudah Menyadap Password \& Pencegahannya*. Jakarta Selatan: Mediakita, 2023.

LAMPIRAN

Lampiran 1 Kuesioner

KUESIONER PENELITIAN

PENGARUH ANCAMAN PHISING DAN PRINSIP KEHATI-HATIAN TERHADAP TINGKAT KEPERCAYAAN NASABAH PENGGUNA MOBILE BANKING

(Pada Mahasiswa Fakultas Ekonomi dan Bisnis Islam UIN Palopo)

Kepada responden yang terhormat,

Assalamu'alaikum Wr. Wb.

Saya atas nama Muh. Fikri Haikal, yang merupakan mahasiswa program studi Perbankan Syariah pada Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri (UIN) Palopo. Saya mohon kesediaan Saudara/i untuk meluangkan waktu untuk mengisi kuesioner yang berkaitan dengan Ancaman *Phising* dan Prinsip Kehati-hatian terhadap Tingkat Kepercayaan Nasabah Pengguna *Mobile Banking* (Pada Mahasiswa Fakultas Ekonomi dan Bisnis Islam UIN Palopo). Adapun tujuan dari kuesioner ini adalah sebagai bahan masukan untuk memperoleh data yang akurat dalam penyusunan skripsi. Oleh sebab itu, mohon Saudara/i mengisi kuesioner dengan sebenar-benarnya. Jawaban yang Saudara/i berikan dalam kuesioner ini akan saya jamin kerahasiaannya karena kuesioner ini hanya digunakan untuk kegiatan penelitian. Atas partisipasi Saudara/i saya ucapkan terima kasih.

Wassamu'alaikum Wr. Wb.

A. Biodata Responden

Isi dan berikan tanda centang () pada kotak yang tersedia dibawah ini:

Nama	:	
Jenis Kelamin	: <input type="checkbox"/> Laki-laki	<input type="checkbox"/> Perempuan
Usia	:	
<input type="checkbox"/> <20 Tahun	<input type="checkbox"/> 20-22 Tahun	<input type="checkbox"/> 22-24 Tahun
	<input type="checkbox"/> 24-25 Tahun	<input type="checkbox"/> >25 Tahun

B. Petunjuk Pengisian

1. Bacalah sejumlah pernyataan dibawah ini dengan teliti.
2. Anda dimohon memberikan penilaian mengenai pengaruh ancaman *Phising*, prinsip kehati-hatian, kepercayaan nasabah terhadap pengguna *Mobile Banking* di bank BSI pada penulisan skripsi.
3. Anda dimohon untuk memberikan jawaban sesuai dengan keadaan secara

objektif dengan memberi tanda centang (✓) pada salah satu kriteria untuk setiap pernyataan yang menurut Anda paling tepat.

4. Skor yang diberikan tidak mengandung nilai jawaban benar-salah melainkan menunjukkan kesesuaian penilaian Anda terhadap isi setiap pernyataan.
5. Pilihan jawaban yang tersedia adalah:

SINGKATAN	KETERANGAN	NILAI
SS	SangatSetuju	5
S	Setuju	4
N	Netral	3
TS	TidakSetuju	2
STS	SangatTidakSetuju	1

6. Dimohon dalam memberikan penilaian tidak ada pernyataan yang terlewatkan.
7. Hasil penelitian ini hanya untuk ke pentingan akademisi saja. identitas anda akan dirahasiakan dan hanya diketahui oleh peneliti.

C. Syarat Pengisian

1. Mahasiswa aktif Fakultas Ekonomi dan Bisnis Islam UIN Palopo.
2. Pengguna aktif *Mobile Banking* minimal 1 bulan terakhir

D. Daftar Pertanyaan

1. Apakah anda pernah/sedang menggunakan *Mobile Banking* dalam 1 bulan terakhir?

YA

TIDAK

2. Apakah anda sudah paham tentang Situs *Phising*?

YA

TIDAK

E. Variabel Ancaman *Phising* (X1)

NO	PERNYATAAN	JAWABAN				
		SS	S	N	TS	STS
		5	4	3	2	1
1	Saya merasa takut dengan adanya rumor tingkat insiden ancaman <i>Phising</i> yang meningkat pada <i>online Mobile Banking</i>					

2	Saya mencari tahu tentang pola serangan pada ancaman <i>Phising</i> di media sosial maupun berita
3	Ancaman <i>Phising</i> dapat disebabkan oleh pelaku <i>cyber</i> yang mengirimkan alamat web palsu ke dalam e-mail/pesan chat dengan menggunakan identitas bank
4	Apabila menerima pesan yang mencurigakan dan meminta untuk melakukan verifikasi registrasi <i>password</i> atau aktivasi data, akan sangat berguna jika kita menghubungi pihak <i>customer service</i> bank secara langsung

F. Variabel Prinsip Kehati-hatian (X2)

NO	PERNYATAAN	JAWABAN				
		SS	S	N	TS	STS
		5	4	3	2	1
1	Saya merasa yakin dan percaya untuk menggunakan <i>Mobile Banking</i> dalam melakukan transaksi perbankan					
2	Saya yakin semua data yang di proses melalui <i>Mobile Banking</i> tidak akan disalah gunakan oleh pihak bank					
3	Saya merasa yakin bahwa keamanan dalam transaksi layanan <i>Mobile Banking</i> akurat					
4	Saya merasa yakin bahwa bank memberikan rasa aman dan menjaga kerahasiaan					

G. Variabel Tingkat Kepercayaan Nasabah (Y)

NO	PERNYATAAN	JAWABAN				
		SS	S	N	TS	STS
		5	4	3	2	1
1	Kerahasiaan data pribadi saya terjamin dalam transaksi <i>Mobile Banking</i>					
2	Bank memberikan jaminan keamanan saldo saya direkening					

-
- 3 Jaminan keamanan dan menjaga kerahasiaan data nasabah dalam bertransaksi pada *Mobile Banking* terjamin keamanannya
-
- 4 Bank memberikan penyuluhan tentang situs *Phising* untuk keamanan dalam bertransaksi melalui *Mobile Banking*
-

Lampiran 2 Hasil Kuesioner

Rspn	Ancaman Phising (X1)				Tot al	Prinsip Kehati-hatian (X2)				Tot al	Tingkat Kepercayaan Nasabah (Y)				
	X1. 1	X1. 2	X1. 3	X1. 4		X2. 1	X2. 2	X2. 3	X2. 4		Y1	Y2	Y3	Y4	Total
1	4	4	4	4	16	4	4	5	5	18	4	4	4	4	16
2	5	5	3	5	18	5	5	4	5	19	4	5	4	4	17
3	5	5	5	5	20	5	5	5	5	20	4	4	5	5	18
4	4	4	5	5	18	4	4	5	5	18	5	4	5	5	19
5	4	4	4	4	16	4	5	5	5	19	5	5	4	4	18
6	5	5	5	5	20	5	4	4	4	17	4	4	5	5	18
7	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
8	5	5	5	5	20	4	5	5	4	18	4	4	5	5	18
9	4	3	3	3	13	3	5	5	4	17	4	4	3	3	14
10	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
11	4	3	4	3	14	3	3	3	3	12	3	3	3	3	12

12	5	5	5	5	20	5	4	4	4	17	4	4	5	5	18
13	5	5	5	5	20	5	3	3	3	14	3	3	5	5	16
14	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
15	4	4	4	4	16	4	3	3	3	13	3	3	4	4	14
16	5	5	5	5	20	5	5	4	5	19	5	5	5	5	20
17	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
18	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
19	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
20	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
21	4	4	5	4	17	4	4	4	4	16	4	4	4	4	16
22	4	4	5	5	18	5	5	5	5	20	5	5	5	5	20
23	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
24	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
25	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
26	5	5	5	5	20	4	5	5	5	19	5	5	5	5	20
27	4	4	5	5	18	5	5	5	5	20	5	5	5	5	20
28	5	5	5	5	20	5	3	3	3	14	3	3	5	5	16
29	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
30	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20

31	4	3	3	3	13	3	5	5	5	18	5	5	3	3	16
32	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
33	4	3	3	3	13	3	4	4	4	15	4	4	3	3	14
34	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
35	5	5	5	4	19	4	5	5	5	19	5	5	5	5	20
36	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
37	4	4	5	5	18	5	5	5	5	20	5	5	5	5	20
38	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
39	5	5	5	5	20	4	5	5	5	19	5	5	3	5	18
40	4	4	4	4	16	4	4	4	4	16	4	4	3	4	15
41	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
42	5	5	5	5	20	5	5	5	5	20	5	5	5	4	19
43	5	5	5	5	20	5	5	5	5	20	5	5	5	4	19
44	4	4	4	4	16	4	5	4	4	17	4	4	4	4	16
45	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
46	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
47	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
48	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
49	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20

50	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
51	5	5	5	5	20	5	5	5	3	18	4	4	4	4	16
52	5	5	5	5	20	5	5	5	4	19	4	4	4	4	16
53	4	4	4	4	16	4	4	4	4	16	5	5	5	5	20
54	5	5	5	4	19	4	5	5	5	19	5	5	5	5	20
55	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
56	5	5	4	4	18	3	5	5	5	18	3	4	4	4	15
57	4	4	4	4	16	4	4	4	4	16	3	4	5	5	17
58	5	5	5	4	19	4	5	5	5	19	5	4	5	5	19
59	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
60	5	5	4	4	18	4	5	5	5	19	4	4	4	4	16
61	4	4	4	3	15	3	4	4	4	15	4	4	4	4	16
62	3	3	3	3	12	3	3	3	3	12	3	3	4	3	13
63	5	5	4	4	18	4	4	3	3	14	3	3	4	3	13
64	5	5	4	4	18	4	4	4	4	16	4	4	4	4	16
65	4	4	4	4	16	4	5	4	4	17	4	4	4	4	16
66	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
67	5	5	4	4	18	3	5	5	5	18	4	4	4	4	16
68	5	5	4	4	18	4	5	5	5	19	4	4	4	4	16

69	4	4	4	4	16	4	5	5	5	19	4	4	4	4	16
70	3	3	3	4	13	4	4	4	4	16	3	3	3	3	12
71	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
72	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
73	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
74	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
75	5	5	5	5	20	5	5	5	5	20	4	4	4	4	16
76	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
77	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
78	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
79	4	4	5	5	18	5	4	4	4	17	4	4	4	4	16
80	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
81	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
82	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
83	4	4	5	5	18	5	4	4	4	17	4	4	4	4	16
84	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
85	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
86	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
87	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20

88	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
89	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
90	4	4	4	4	16	4	4	4	4	16	5	5	5	5	20
91	4	4	5	5	18	5	4	4	4	17	4	4	4	4	16
92	5	5	4	4	18	4	5	5	5	19	5	5	5	5	20
93	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
94	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16
95	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
96	4	4	5	5	18	4	4	4	4	16	4	4	4	4	16
97	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
98	4	4	5	5	18	5	4	4	4	17	4	4	4	4	16
99	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20
100	4	4	4	4	16	4	4	4	4	16	5	5	5	5	20

Lampiran 3 hasil Olah Data Kuesioner

a. Uji Relibilitas

Correlations

		X1.1	X1.2	X1.3	X1.4	ancaman_phising_X1
X1.1	Pearson Correlation	1	.949**	.492**	.485**	.842**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	100	100	100	100	100
X1.2	Pearson Correlation	.949**	1	.561**	.580**	.893**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	100	100	100	100	100
X1.3	Pearson Correlation	.492**	.561**	1	.849**	.850**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	100	100	100	100	100
X1.4	Pearson Correlation	.485**	.580**	.849**	1	.854**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	100	100	100	100	100
ancaman_phising_X1	Pearson Correlation	.842**	.893**	.850**	.854**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	100	100	100	100	100

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

Correlations

		X2.1	X2.2	X2.3	X2.4	prinsip_kehati_hatian_X2
X2.1	Pearson Correlation	1	.287**	.251*	.269**	.550**
	Sig. (2-tailed)		.004	.012	.007	.000
	N	100	100	100	100	100
X2.2	Pearson Correlation	.287**	1	.904**	.844**	.918**
	Sig. (2-tailed)	.004		.000	.000	.000
	N	100	100	100	100	100
X2.3	Pearson Correlation	.251*	.904**	1	.883**	.920**
	Sig. (2-tailed)	.012	.000		.000	.000
	N	100	100	100	100	100
X2.4	Pearson Correlation	.269**	.844**	.883**	1	.909**
	Correlation					

	Sig. (2-tailed)	.007	.000	.000		.000
	N	100	100	100	100	100
prinsip_kehati_hatian_X2	Pearson Correlation	.550**	.918**	.920**	.909**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	100	100	100	100	100

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

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

Correlations

		Y1	Y2	Y3	Y4	tingkat_Kepercayaan_X3
Y1	Pearson Correlation	1	.939**	.610**	.670**	.904**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	100	100	100	100	100
Y2	Pearson Correlation	.939**	1	.602**	.665**	.899**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	100	100	100	100	100
Y3	Pearson Correlation	.610**	.602**	1	.884**	.866**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	100	100	100	100	100
Y4	Pearson Correlation	.670**	.665**	.884**	1	.901**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	100	100	100	100	100
tingkat_Kepercayaan_X3	Pearson Correlation	.904**	.899**	.866**	.901**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	100	100	100	100	100

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

b. Uji Reliabilitas

Reliability Statistics

Cronbach's	
Alpha	N of Items
.882	4

Reliability Statistics

Cronbach's	
Alpha	N of Items
.842	4

Reliability Statistics

Cronbach's	
Alpha	N of Items
.915	4

c. Uji Normalitas

One-Sample Kolmogorov-Smirnov Test

		Unstandardized Residual
N		100
Normal Parameters ^{a,b}	Mean	.0000000
	Std. Deviation	1.35135473
Most Extreme Differences	Absolute	.189
	Positive	.137
	Negative	-.189
Test Statistic		1.189
Asymp. Sig. (2-tailed)		.077 ^c

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

d. Uji Multikolinearitas

Coefficients^a

Model	Collinearity Statistics	
	Tolerance	VIF
1_ancaman_phising_X1	.520	1.922
prinsip_kehati_hatian_X2	.520	1.922

a. Dependent Variable: tingkat_Kepercayaan_X3

e. Uji Heterokedastisitas

Coefficients^a

Model	Unstandardized Coefficients		Standardized Coefficients Beta	t	Sig.
	B	Std. Error			
1 (Constant)	1.485	.949		1.564	.121
ancaman_phising_X1	-.111	.067	-.229	-1.648	.103
prinsip_kehati_hatian_X2	.079	.068	.163	1.173	.244

a. Dependent Variable: abs_res

f. Uji Regresi Linear Berganda Dan Uji T

Coefficients^a

Model	Unstandardized Coefficients		Standardized Coefficients Beta	t	Sig.
	B	Std. Error			
1 (Constant)	.700	1.325		.528	.599
ancaman_phising_X1	.254	.094	.228	2.711	.008
prinsip_kehati_hatian_X2	.700	.094	.626	7.422	.000

a. Dependent Variable: tingkat_Kepercayaan_X3

g. Uji F

ANOVA^a

Model	Sum of Squares	df	Mean Square	F	Sig.
1 Regression	323.450	2	161.725	86.771	.000 ^b
Residual	180.790	97	1.864		
Total	504.240	99			

a. Dependent Variable: tingkat_Kepercayaan_X3

b. Predictors: (Constant), prinsip_kehati_hatian_X2, ancaman_phising_X1

h. Uji R

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.801 ^a	.641	.634	1.36522

a. Predictors: (Constant), prinsip_kehati_hatian_X2, ancaman_phising_X1

Lampiran 4 F tabel

Titik Persentase Distribusi F untuk Probabilita = 0,05

df untuk penyebut (N2)	df untuk pembilang (N1)														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
91	3.95	3.10	2.70	2.47	2.31	2.20	2.11	2.04	1.98	1.94	1.90	1.86	1.83	1.80	1.78
92	3.94	3.10	2.70	2.47	2.31	2.20	2.11	2.04	1.98	1.94	1.89	1.86	1.83	1.80	1.78
93	3.94	3.09	2.70	2.47	2.31	2.20	2.11	2.04	1.98	1.93	1.89	1.86	1.83	1.80	1.78
94	3.94	3.09	2.70	2.47	2.31	2.20	2.11	2.04	1.98	1.93	1.89	1.86	1.83	1.80	1.77
95	3.94	3.09	2.70	2.47	2.31	2.20	2.11	2.04	1.98	1.93	1.89	1.86	1.82	1.80	1.77
96	3.94	3.09	2.70	2.47	2.31	2.19	2.11	2.04	1.98	1.93	1.89	1.85	1.82	1.80	1.77
97	3.94	3.09	2.70	2.47	2.31	2.19	2.11	2.04	1.98	1.93	1.89	1.85	1.82	1.80	1.77
98	3.94	3.09	2.70	2.46	2.31	2.19	2.10	2.03	1.98	1.93	1.89	1.85	1.82	1.79	1.77
99	3.94	3.09	2.70	2.46	2.31	2.19	2.10	2.03	1.98	1.93	1.89	1.85	1.82	1.79	1.77
100	3.94	3.09	2.70	2.46	2.31	2.19	2.10	2.03	1.97	1.93	1.89	1.85	1.82	1.79	1.77
101	3.94	3.09	2.69	2.46	2.30	2.19	2.10	2.03	1.97	1.93	1.88	1.85	1.82	1.79	1.77
102	3.93	3.09	2.69	2.46	2.30	2.19	2.10	2.03	1.97	1.92	1.88	1.85	1.82	1.79	1.77
103	3.93	3.08	2.69	2.46	2.30	2.19	2.10	2.03	1.97	1.92	1.88	1.85	1.82	1.79	1.76
104	3.93	3.08	2.69	2.46	2.30	2.19	2.10	2.03	1.97	1.92	1.88	1.85	1.82	1.79	1.76
105	3.93	3.08	2.69	2.46	2.30	2.19	2.10	2.03	1.97	1.92	1.88	1.85	1.81	1.79	1.76
106	3.93	3.08	2.69	2.46	2.30	2.19	2.10	2.03	1.97	1.92	1.88	1.84	1.81	1.79	1.76
107	3.93	3.08	2.69	2.46	2.30	2.18	2.10	2.03	1.97	1.92	1.88	1.84	1.81	1.79	1.76
108	3.93	3.08	2.69	2.46	2.30	2.18	2.10	2.03	1.97	1.92	1.88	1.84	1.81	1.78	1.76
109	3.93	3.08	2.69	2.45	2.30	2.18	2.09	2.02	1.97	1.92	1.88	1.84	1.81	1.78	1.76
110	3.93	3.08	2.69	2.45	2.30	2.18	2.09	2.02	1.97	1.92	1.88	1.84	1.81	1.78	1.76

Lampiran 6 R Tabel

Tabel Nilai r Product Moment

N	Taraf Signif		N	Taraf Signif		N	Taraf Signif	
	5%	10%		5%	10%		5%	10%
3	0,997	0,999	27	0,381	0,487	55	0,266	0,345
4	0,950	0,990	28	0,374	0,478	60	0,254	0,330
5	0,878	0,959	29	0,367	0,470	65	0,244	0,317
6	0,811	0,917	30	0,361	0,463	70	0,235	0,306
7	0,754	0,874	31	0,355	0,456	75	0,227	0,296
8	0,707	0,834	32	0,349	0,449	80	0,220	0,286
9	0,666	0,798	33	0,344	0,442	85	0,213	0,278
10	0,632	0,765	34	0,339	0,436	90	0,207	0,270
11	0,602	0,735	35	0,334	0,430	95	0,202	0,263
12	0,576	0,708	36	0,329	0,424	100	0,195	0,256
13	0,553	0,684	37	0,325	0,418	125	0,176	0,230
14	0,532	0,661	38	0,320	0,413	150	0,159	0,210
15	0,514	0,641	39	0,316	0,408	175	0,148	0,194
16	0,497	0,623	40	0,312	0,403	200	0,138	0,181
17	0,482	0,606	41	0,308	0,398	300	0,113	0,148
18	0,468	0,590	42	0,304	0,393	400	0,098	0,128
19	0,456	0,575	43	0,301	0,389	500	0,088	0,115
20	0,444	0,561	44	0,297	0,384	600	0,080	0,105
21	0,433	0,549	45	0,294	0,380	700	0,074	0,097
22	0,423	0,537	46	0,291	0,376	800	0,070	0,091
23	0,413	0,526	47	0,288	0,372	900	0,065	0,086
24	0,404	0,515	48	0,284	0,368	1000	0,062	0,081
25	0,396	0,505	49	0,281	0,364			
26	0,388	0,496	50	0,279	0,361			

DAFTAR RIWAYAT HIDUP



Muh. Fikri Haikal, Lahir Pada 04 Januari 2002 Di Palopo, Sulawesi Selatan. Penulis Adalah Anak Pertama Dari 3 Bersaudara, Dengan Ayah Bernama Supri Dan Ibu Bernama Sarimaya. Saat Ini Penulis Tinggal Di Palopo, Perumnas Benteng Raya Blok B No.34, Kecamatan Wara Timur, Kabupaten Kota Palopo. Pendidikan Dasar Diselesaikan Pada Tahun 2014 di SDN 1 Lalebbata. Dan Pada Tahun Yang Sama Penulis Melanjutkan Pendidikan di MtsN Kota Palopo Hingga 2017. Setelah Itu, Penulis Melanjutkan Studi di SMAN 3 Palopo dan Lulus Pada Tahun 2020. Setelah Lulus SMA, Penulis Melanjutkan Pendidikan di Bidang Perbankan Syariah di Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri (UIN) Kota Palopo.

Contact Person:

20104200031@uinpalopo.ac.id