PENGARUH PRINSIP KEHATI-HATIAN TERHADAP ANCAMAN SITUS PHISHING PADA NASABAH PENGGUNA INTERNET *BANKING*
(Studi Kasus Pada Bank Syariah di Kota Palopo)

Skripsi

Diajukan untuk Memenuhi Salah Satu Syarat Guna Memperoleh Gelar Sarjana Ekonomi (SE) pada Program Studi Perbankan Syariah Fakultas Ekonomi dan Bisnis Islam Institut Agama Islam Negeri Palopo

IAIN PALOPO

Oleh

ANDI SITI NURBAYA SARI
16 0402 0013

PROGRAM STUDI PERBANKAN SYARIAH
FAKULTAS EKONOMI DAN BISNIS ISLAM
INSTITUT AGAMA ISLAM NEGERI PALOPO
2021

PENGARUH PRINSIP KEHATI-HATIAN TERHADAP ANCAMAN SITUS PHISHING PADA NASABAH PENGGUNA INTERNET *BANKING*
(Studi Kasus Pada Bank Syariah di Kota Palopo)

Skripsi

Diajukan untuk Memenuhi Salah Satu Syarat Guna Memperoleh Gelar Sarjana Ekonomi (SE) pada Program Studi Perbankan Syariah Fakultas Ekonomi dan Bisnis Islam Institut Agama Islam Negeri Palopo

IAIN PALOPO

Oleh

ANDI SITI NURBAYA SARI
16 0402 0013

Pembimbing:

1. **Burhan Rifuddin, SE., M.M.**
2. **Hendra Safri, SE., M.M.**

PROGRAM STUDI PERBANKAN SYARIAH
FAKULTAS EKONOMI DAN BISNIS ISLAM
INSTITUT AGAMA ISLAM NEGERI PALOPO
2021

HALAMAN PERNYATAAN KEASLIAN

Saya yang bertandatangan di bawah ini:

Nama	: Aisyah A. Haeruddin
NIM	: 16 0402 0010
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/tesis ini adalah karya saya sendiri selain kutipan yang ditunjukkan sumbernya. Segala kekeliruan dan atau kesalahan yang ada di dalamnya adalah tanggungjawab saya.

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

Demikian pernyataan ini dibuat untuk dipergunakan sebagaimana mestinya.

Palopo, 17 Maret 2021

Yang membuat pernyataan,

Aisyah A. Haeruddin

NIM 16 0402 0010

HALAMAN PENGESAHAN

Skripsi berjudul Implementasi Pembiayaan Murabahah di BSM Palopo yang ditulis oleh Aisyah A. Haeruddin Nomor Induk Mahasiswa (NIM) 16 0402 0010, mahasiswa Program Studi Perbankan Syariah Fakultas Ekonomi dan Bisnis Islam Institut Agama Islam Negeri Palopo, yang dimunaqasyahkan pada hari Rabu tanggal 05 Mei 2021 miladiyah bertepatan dengan 23 Ramadhan 1442 hijriyah telah diperbaiki sesuai catatan dan permintaan Tim Penguji, dan diterima sebagai syarat meraih gelar Sarjana Ekonomi (S.E).

Palopo, 10 Mei 2021

TIM PENGUJI

1.	Dr. Hj. Ramlah M., M.M.	Ketua Sidang	(.....)
2.	Tadjuddin,SE.,M.Si.,Ak.,CA.,CSRS.,CAPF.,CSRA.	Sekertaris Sidang	(.....)
3.	Dr. Muh. Ruslan Abdullah, S.E.I.,M.A.	Penguji I	(.....)
4.	Dr. Fasiha S.E.I.,M.E.I.	Penguji II	(.....)
5.	Ilham, S.Ag., M.A.	Pembimbing I	(.....)
6.	Nurdin Batjo, S.Pt., M.M.	Pembimbing II	(.....)

Mengetahui:

a.n Rektor IAIN Palopo	Ketua Program Studi
Dekan Fakultas Ekonomi dan Bisnis Islam	Perbankan Syariah
Dr. Hj. Ramlah M., M.M.	**Hendra Safri, S.E., M.M.**
NIP.19610208 199403 2 001	NIP.19861020 201503 1 001

PRAKATA

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْمِ

اَلْحَمْدُ لِلّٰهِ رَبِّ الْعَالَمِيْنَ وَالصَّلَاةُ وَالسَّلَامُ عَلَى اَشْرَفِ الْاَنْبِيَاءِ وَالْمُرْسَلِيْنَ سَيِّدِنَا مُحَمَّدٍ وَعَلَى اٰلِهِ وَاَصْحَابِهِ اَجْمَعِيْنَ

Segala puji dan syukur penulis panjatkan kepada Allah SWT. yang telah menganugerahkan rahmat dan hidayahnya sehingga penulis dapat menyelesaikan penulisan skripsi ini dengan judul "Pengaruh Prinsip Kehati-hatian Terhadap Ancaman Situs Phishing Pada Nasabah Pengguna Internet Banking" dapat terselesaikan dengan baik .

Selawat serta salam penulis haturkan kepada Baginda Muhammad SAW. kepada para keluarga, sahabat serta pengikut-pengikutnya hingga akhir zaman.

Perjalanan panjang telah penulis lalui dalam rangka perampungan penulisan skripsi ini. Banyak hambatan yang dihadapi dalam penyusunannya, namun dapat terselesaikan berkat bantuan, bimbingan serta dorongan dari banyak pihak baik moril maupun materil walaupun penulisan skripsi ini masih jauh dari kata sempurna. Oleh karena itu, dengan penuh kerendahan hati pada kesempatan ini patutlah kiranya penulis menyampaikan terima kasih yang tak terhingga terkhusus kepada orang tua penulis tercinta, Ibunda A. St Asminiadi dan Alm. Bapak S. Bahrir, serta Nenek penulis Opu Superi yang telah sabar mengasuh dan mendidik penulis serta senantiasa mendoakan untuk kelancaran studi penulis. Serta ucapan terima kasih yang tak terhingga kepada:

1. Wakil Rektor Bidang Akademik dan Kelembagaan, Dr. H. Muammar Arafat, M.H. Wakil Rektor Bidang Administrasi Umum,Perencanaan dan Keuangan, Dr. Ahmad Syarief Iskandar, S.E., M.M. Wakil Rektor Bidang

Kemahasiswaan dan Kerjasama, Dr. Muhaemin, M.A. yang telah membina dan berupaya meningkatkan mutu perguruan tinggi ini, tempat penulis menimba ilmu pengetahuan.

2. Dekan Fakultas Ekonomi dan Bisnis Islam IAIN Palopo, Dr. Hj. Ramlah Makkulasse, M.M. Wakil Dekan Bidang Akademik Muh. Ruslan Abdullah, S.E.I., M.A. Wakil Dekan Bidang Adm. Umum, Perencanaan dan Keuangan Tadjuddin, S.E., M.Si., Ak., CA. Wakil Dekan Bidang Kemahasiswaan dan Kerjasama Dr. Takdir, S.H., M.H yang telah banyak memberikan motivasi serta mencurahkan perhatiannya dalam membimbing dan memberikan petunjuk sehingga skripsi ini dapat terselesaikan.
3. Ketua Program Studi Perbankan Syariah, Hendra Safri, S.E., M.M, Sekretaris Program Studi Perbankan Syariah, Nur Ariani Aqidah, S.E.,M.Sc. Para dosen beserta seluruh staf pegawai IAIN Palopo yang telah mendidik penulis selama berada di IAIN Palopo dan memberikan bantuan dalam penyusunan skripsi ini.
4. Dosen Penasehat Akademik (PA), Dr. Takdir, S.H.,M.H yang telah mendidik penulis selama berada di IAIN Palopo dan memberikan bantuan dalam penyusunan skripsi ini.
5. Dosen Pembimbing I, Burhan Rifuddin, M.M dan Dosen Pembimbing II, Hendra Safri, M.M. yang telah memberikan arahan dan bimbingan kepada penulis dengan tulus dalam menyelesaikan skripsi ini.
6. Dosen Penguji I, Dr. Mahadin Shaleh, M.Si. dan Dosen Penguji II, Dr. Mujahidin Lc.,M.E.I. yang telah memberikan arahan dan bimbingan kepada penulis dengan tulus dalam menyelesaikan skripsi ini.

7. Kepala Perpustakaan dan segenap karyawan dan karyawati dalam ruang lingkup IAIN Palopo, yang telah memberikan peluang untuk penulis dalam mengumpulkan literatur yang berkaitan dengan pembahasan skripsi ini.
8. Kepada kakak-kakak HMPS Perbankan Syariah periode 2018, dan juga Kakanda Erwin, S,E yang telah membimbing dan memberi arahan kepada penulis dalam penyelesaian skripsi ini.
9. Sahabat PDKT Aisyah A. Haeruddin, Afriyanti M dan Armila. Sahabat Maccarita 3 Maruf, Anzal, Isva, Vera, Inar, Rama, Saiful, Tenri, Maudy, Ani,Aksal, Gaffar, Fira, Tiwi, Biduan ku Nurbaeti Samari, Andalangku Cahaya ,Febi dan Regina. yang selalu senantiasa setia menemani dan mendukung, berbagi pikiran, dan telah rela mengorbankan tenaga dan waktunya untuk membantu penulis dalam menyelesaikan skripsi ini.
10. Keluarga besar Kelompok Studi Ekonomi Islam (KSEI) Sharia Economic Association (SEA), Forum Silaturahim Studi Ekonomi Islam (FoSSEI) Sulawesi Selatan Barat dan Papua yang telah mendoakan penulis sehingga skripsi ini dapat terselesaikan.
11. Kepada semua teman seperjuangan Perbankan Syariah Angkatan 2016 (khususnya kelas A) yang sudah membantu serta senantiasa memberikan saran sehubungan dengan penyusunan skripsi ini.

Teriring doa, semoga amal kebaikan serta keikhlasan pengorbanan mereka mendapat pahala yang setimpal dari Allah swt. dan selalu diberi petunjuk ke jalan yang lurus serta mendapat Ridho-Nya amin.

Penulis menyadari sepenuhnya bahwa skripsi ini masih jauh dari kesempurnaan karena keterbatasan pengalaman dan pengetahuan yang dimiliki penulis. Oleh karena itu, penulis mengharapkan segala bentuk saran serta masukan bahkan kritik yang membangun dari berbagai pihak.

Palopo, 11 April 2021

Penulis

PEDOMAN TRANSLITERASI ARAB-LATIN DAN SINGKATAN

A. Transliterasi Arab-Latin

Daftar huruf bahasa Arab dan transliterasinya ke dalam huruf Latin dapat dilihat pada tabel berikut:

1. Konsonan

Huruf Arab	Nama	Huruf Latin	Nama
ا	Alif	-	-
ب	Ba’	B	Be
ت	Ta’	T	Te
ث	Ṡa’	Ṡ	Es dengan titik di atas
ج	Jim	J	Je
ح	Ḥa’	Ḥ	Ha dengan titik di bawah
خ	Kha	Kh	Ka dan ha
د	Dal	D	De
ذ	Żal	Ż	Zet dengan titik di atas
ر	Ra’	R	Er
ز	Zai	Z	Zet
س	Sin	S	Es
ش	Syin	Sy	Esdan ye
ص	Ṣad	Ṣ	Es dengan titik di bawah
ض	Ḍaḍ	Ḍ	De dengan titik di bawah
ط	Ṭa	Ṭ	Te dengan titik di bawah
ظ	Ẓa	Ẓ	Zet dengan titik di bawah
ع	‘Ain	‘	Koma terbalik di atas
غ	Gain	G	Ge
ف	Fa	F	Fa
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

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 bahasa Arab, seperti vokal bahasa Indonesia, terdiri atas vokal tunggal atau monoftong dan vokal rangkap atau diftong.

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

Tanda	Nama	Huruf Latin	Nama
أَ	*fatḥah*	a	a
إِ	*kasrah*	i	i
أُ	*ḍammah*	u	u

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

Tanda	Nama	Huruf Latin	Nama
ـَيْ	*fatḥah dan yā’*	ai	a dan i
ـَوْ	*fatḥah* dan *wau*	au	a dan u

Contoh:

كَيْفَ : *kaifa*

هَوْ لَ : *haula*

3. *Maddah*

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

Harakat dan Huruf	Nama	Huruf dan Tanda	Nama
ى َ... | ا َ...	*fatḥah* dan *alif* atau *yā'*	ā	a dan garis di atas
ِ ي	*kasrah* dan *yā'*	ī	i dan garis di atas
ُ و	*ḍammah* dan *wau*	ū	u dan garis di atas

مَاتَ : māta

رَمَى : rāmā

قِيْلَ : qīla

يَمُوْتُ : 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]. sedangkan *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:

رَوْضَةُ الأَطْفَالِ : *raudah al-atfāl*

اَلْمَدِيْنَةُ اَلْفَاضِلَةُ : *al-madīnah al-fādilah*

اَلْحِكْمَةُ : *al-hikmah*

5. Syaddah *(Tasydīd)*

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

Contoh:

رَبَّنَا : *rabbanā*

نَجَّيْنَا : *najjainā*

اَلْحَقّ : *al-haqq*

نُعِّمَ : *nu'ima*

عَدُوٌّ : *'aduwwun*

Jika huruf ى ber-*tasydid* di akhir sebuah kata dan didahului oleh huruf *kasrah* (ـِـيّ), 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:

اَلشَّمْسُ	: *al-syamsu* (bukan *asy-syamsu*)
اَلزَّلْزَلَة	: *al-zalzalah* (bukan *az-zalzalah*)
اَلْفَلْسَفَة	: *al-falsafah*
اَلْبِلَادُ	: *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:

تَأْمُرُوْنَ	: *ta’murūna*
اَلنَّوْعُ	: *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 fi Ri'āyah al-Maslahah

9. *Lafz al-Jalālah*

Kata "Allah" yang didahului partikel seperti huruf jarr dan huruf lainnya atau berkedudukan sebagai *mudāf ilaih* (frasa nominal), ditransliterasi tanpa huruf hamzah.

Contoh:

دِيْنُ اللهِ *dīnullāh* بِاللهِ *billāh*

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

هُمْ فِيْ رَحْمَةِ اللهِ *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

B. Daftar *Singkatan*

Beberapa singkatan yang dibakukan adalah:

SWT.	= Subhanahu Wa Ta'ala
SAW.	= Sallallahu 'Alaihi Wasallam
AS	= 'Alaihi Al-Salam
H	= Hijrah
M	= Masehi
SM	= Sebelum Masehi
l	= Lahir Tahun (untuk orang yang masih hidup saja)
W	= Wafat Tahun
QS …/…: 4	= QS al-Baqarah/2: 4 atau QS Ali 'Imran/3: 4
HR	= Hadis Riwayat

DAFTAR ISI

DAFTAR KUTIPAN AYAT

DAFTAR HADIST

DAFTAR TABEL

DAFTAR GAMBAR

ABSTRAK

Andi Siti Nurbaya Sari, 2021. "Pengaruh Prinsip Kehati-hatian terhadap Ancaman Situs Phishing Pada Nasabah Pengguna Internet Banking". Skripsi Program Studi Perbankan Syariah, Fakultas Ekonomi dan Bisnis Islam. Pembimbing I Burhan Rifuddin, S.E.,M.M. dan Pembimbing II Hendra Safri, S.E.,M.M.

Skripsi ini menjelaskan tentang pengaruh prinsip kehati-hatian terhadap ancaman situs *phishing* pada nasabah pengguna internet banking. Masalah utama dalam penelitian ini yaitu adanya sebuah situs internet yang merujuk pada tindakan memancing pengguna internet banking untuk mengunjungi situs Web palsu rancangan para *cyber* yang sedemikian rupa menyerupai situs resminya untuk mengelabui korbannya melalui email palsu (atau pesan instan) kemudian secara diam-diam mengambil informasi pribadi korban. Melihat hal tersebut diperlukan prinsip kehati-hatian yang diatur oleh perbankan untuk mengetahui identitas nasabah, memantau kegiatan transaksi nasabah termasuk pelaporan transaksi yang mencurigakan.

Jenis penelitian yang digunakan ialah Metode Kuantitatif. Penelitian ini menggunakan 30 sampel dengan menggunakan teknik penarikan sampel *nonprobability* 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 internet banking di bank syariah kota palopo.

Kata Kunci : Situs Phising, Prinsip Kehati-hatian, Internet

BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Dikala ini perbankan di dunia telah memakai teknologi mutahir, dimana bisa di akses lewat internet ataupun jejaring sosial yang lain. Memandang perihal ini, bank pemerintah serta bank swasta mengambil kesempatan dengan memandang persaingan kedepannya.[1] Dampak mutahir yang dihasilkannya seperti itu membuat Internet jadi eksis dalam perdagangan elektronik. Timbulnya perbankan internet sudah membuat bank berpikir ulang sistem TI mereka supaya senantiasa kompetitif sebab layanan perbankan Internet diyakini sangat berarti untuk eksistensi masa depan bank-bank di dunia industri elektronik. Serta diprediksikan Indonesia ialah satu antara lain yang hendak jadi pasar digital terbanyak ASEAN di tahun 2020, perihal ini yang dikemukakan oleh World Economic Forum (2015).

Perihal ini mempertegas kesempatan inklusi keuangan digital, diperkuat dengan statment Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menuliskan sebesar 171,17 juta warga Indonesia sudah mengakses internet, berkat infrastruktur yang tumbuh serta smartphone bisa di peroleh dimana saja. Tidak hanya itu bersumber pada hasil kajian Jenius Financial Study: Indonesia Digital Savvy Behavior yang berkolaborasi dengan

[1] Gilang Reski Amijaya, "*Pengaruh Persepsi Teknologi Informasi, Kemudahan, Risiko, dan Fitur Layanan Terhadap Minat Ulang Nasabah Bank Dalam Menggunakan Internet Banking*", *Skripsi* (Semarang: Universitas Diponegoro, 2010): 3.

Nielsen, jumlah nasabah pengguna e-banking bertumbuh dari 23% pada tahun 2014 jadi 36% pada 2018. Dari perkembangan jumlah nasabah tersebut, pengguna internet serta mobile banking pula bertumbuh dari 28% pada 2014 jadi 30% pada 2018. Serta dikala ini telah dilaunchingkan *fintech* lending buat Bank dengan mempraktikkan Digital Branch yang ialah kantor cabang bank yang full digital. Nasabah dengan mandiri melaksanakan transaksi keuangan pada tiap digital branch secara personal serta warga di daerah terpencil yang tidak dapat di pantau perbankan bisa dijangkau.[2]

Dengan demikian, internet banking memungkinkan bank untuk menyediakan layanan ini dengan mengeksploitasi infrastruktur jaringan publik yang luas serta adanya kebutuhan bank untuk menciptakan harmonisasi dan koordinasi yang lebih besar dengan tujuan bisnis bank.[3] Meskipun banyak pekerjaan telah dilakukan di beberapa bank dalam mengadopsi langkah-langkah keamanan dan peraturan *e-banking*, kewaspadaan dan pengelolaan terus menerus akan menjadi penting karena ruang lingkup *e-banking* meningkat. Sebagaimana pentingnya meningkatkan keamanan dalam sistem informasi karena sistem ini menjadi sensitif terhadap lingkungan dan dapat membuat organisasi sangat rentan

[2] Abdus Salam DZ, "Inklusi Keuangan Perbankan Syariah Berbasis Digital-Banking: Optimalisasi dan Tantangan", *Al-Amwal* Vol. 10, no. 1 (2018) : 64-65, http://syekhnurjati.ac.id/jurnal/index.php/amwal/article/view/2813.

[3] Ioannis V. Koskosas, "E-Banking Security : A Communication Perspective", *Risk Management* Vol 13, No. ½ (Greece April 2011): 83, https://www.researchgate.net/publication/261945762_Ebanking_security_A_communication_perspective.

terhadap serangan sistem. Dengan demikian, masalah keamanan dalam konteks internet banking adalah kandidat yang menarik untuk diselidiki.[4]

Walaupun kemampuan khasiat yang ditawarkan internet banking kepada nasabah penerimaan layanannya sudah terbatas serta dalam banyak permasalahan kandas penuhi harapan,[5] diprediksi perihal tersebut diakibatkan oleh ancaman *cybercrime* yang pastinya hendak membagikan akibat kurang baik pada nasabah. Salah satu ancaman yang bisa terjalin ialah terdapatnya web *Phishing* (Password Harvesting). *Phishing* merupakan kata baru yang dihasilkan dari *Fishing* ataupun memancing ini merujuk pada aksi penyerang yang menarik pengguna buat mendatangi website palsu dengan mengirimi mereka email palsu (ataupun pesan praktis) serta secara diam-diam memperoleh data individu korban. Dalam email-email ini, mereka hendak membuat sebagian pemicu, misalnya kata sandi kartu kredit kamu sudah salah dimasukkan berulang kali, ataupun mereka membagikan layanan kenaikan buat meyakinkan kamu mendatangi website mereka buat membiasakan ataupun memodifikasi *no account*

[4] Ioannis V. Koskosas, "Trust and Risk Communication in Setting Internet Banking Security Goals", *Risk Management* Vol 10, No. 1 (Greece Februari 2008): 59-60, https://www.researchgate.net/publication/32042765_Trust_and_Risk_Communication_in_Setting_Internet_Banking_Security_Goals.

[5] Ilmudeen Aboobucker, Yukun Bao, "What Obstruct Costomer Acceptance of Internet Banking? Security and Privacy, Risk, Trust and Website Usability and The Role of Moderators", *Journal of High Technology Management Research, xxx (xxxx) xxx-xxx* (2018): 2, https://www.researchgate.net/publication/324777661_What_obstruct_customer_acceptance_of_internet_banking_Security_and_privacy_risk_trust_and_website_usability_and_the_role_of_moderators.

kamu serta kata sandi lewat hyperlink yang disediakan dalam email.[6]

Masalah ini terjadi pada beberapa bank seperti BCA dan Bank Mandiri, yang menjadi korban dari bank-bank tersebut telah mengalami transaksi palsu pihak ketiga sehingga nasabah mengalami kerugian finansial, bahkan lebih parah lagi, hingga informasi pribadinya bocor. Melihat hal tersebut, tentunya perlu dicermati prinsip kehati-hatian dalam pengawasan bank. Prinsip kehati-hatian sering kali diartikan secara sempit karena hanya melihat kehati-hatian dalam memberikan pembiayaan. Penerapan prinsip kehati-hatian terbagi menjadi tiga yaitu kehati-hatian terhadap lembaga keuangan syariah itu sendiri, kehati-hatian dalam memberikan pembiayaan, dan kehati-hatian yang dibebankan kepada organ perusahaan dalam menjaga kepercayaan nasabah. Menjaga dan meningkatkan kepercayaan masyarakat terhadap produk dan layanan perbankan yang patuh terhadap prinsip syariah merupakan salah satu cara untuk mempercepat pertumbuhan perbankan syariah.

Tata kelola perusahaan syariah yang baik (*Islamic Corporate Governance*) merupakan salah satu cara untuk menjalankan prinsip kehati-hatian dalam memberikan kepercayaan kepada masyarakat dan telah sesuai ketentuan-ketentuan syariah. Dengan telah menerapkan prinsip syariah secara tidak langsung telah melaksanakan bagian dari

[6] E.konda Reddy, dkk, "Detecting Of E-Banking Phishing Websites," *International Journal of Modern Engineering Research (IJMER)* Vol. 2, no. 1 (2012): 46. http://www.ijmer.com/papers/vol2_issue1/I021046054.pdf.

prinsip kehati-hatian. Kehati-hatian sendiri berguna untuk menanggulangi risiko yang mungkin akan terjadi dalam lembaga keuangan syariah. Prinsip yang dianut bank adalah mengidentifikasi nasabah dan memantau aktivitas transaksi nasabah, termasuk melaporkan transaksi yang mencurigakan.[7]

Adapun landasan penerapan prinsip kehati-hatian bank diatur dalam POJK No. 38 tahun 2016 pasal 23 ayat 3 (huruf a) yakni penyelenggaraan pemrosesan transaksi berbasis teknologi Informasi oleh pihak penyedia jasa sebagaimana dimaksud dalam ayat (2) dapat dilakukan sepanjang memenuhi prinsip kehati-hatian.[8] Selain itu prinsip kehati-hatian bagi bank berguna untuk melindungi data nasabah serta terhindar dari praktik-praktik penipuan.[9]

Prinsip kehati-hatian secara umum diperbolehkan berdasarkan Al-Qur'an surah Al Maidah/5 - 49 :

وَأَنِ ٱحۡكُم بَيۡنَهُم بِمَآ أَنزَلَ ٱللَّهُ وَلَا تَتَّبِعۡ أَهۡوَآءَهُمۡ وَٱحۡذَرۡهُمۡ أَن يَفۡتِنُوكَ عَنۢ بَعۡضِ مَآ أَنزَلَ ٱللَّهُ إِلَيۡكَۖ فَإِن تَوَلَّوۡاْ فَٱعۡلَمۡ أَنَّمَا يُرِيدُ ٱللَّهُ أَن يُصِيبَهُم بِبَعۡضِ ذُنُوبِهِمۡۗ وَإِنَّ كَثِيرٗا مِّنَ ٱلنَّاسِ لَفَٰسِقُونَ ٤٩

[7] Asep Rozali, "Prinsip Mengenal Nasabah (Know Your Costumer Principle) Dalam Praktik Perbankan", *Jurnal Wawasan Hukum, Vol. 24 no. 1 (2011)*: 304. http://ejournal.sthb.ac.id/index.php/jwy/article/download/18.

[8] Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Oleh Bank Umum: 23.

[9] Muammar Arafat Yusmad, *Aspek Hukum Perbankan Syariah Dari Teori Ke Praktik*, Ed.1 Cet. 1, (Yogyakarta: Deepublish, 2017), 30.

Terjemahan: *"Dan hendaklah engkau memutuskan perkara di antara mereka menurut apa yang diturunkan Allah, dan janganlah engkau mengikuti keinginan mereka. Dan waspadalah terhadap mereka, jangan sampai mereka memperdayakan engkau terhadap sebagian apa yang telah diturunkan Allah kepadamu. Jika mereka berpaling (dari hukum yang telah diturunkan Allah), maka ketahuilah bahwa sesungguhnya Allah berkehendak menimpakan musibah kepada mereka disebabkan sebagian dosa-dosa mereka. Dan sungguh, kebanyakan manusia adalah orang-orang yang fasik"* [10]

Selain itu dalam hukum islam telah disebutkan dalil tentang merugikan orang lain. Hadist ini membicarakan tentang sikap dan perbuatan seseorang yang membawa mudharat. Hadist yang dimaksud berbunyi:

حَدَّثَنِي يَحْيَى عَنْ مَالِك عَنْ عَمْرِو بْنِ يَحْيَى الْمَازِنِيِّ عَنْ أَبِيهِ أَنَّ رَسُولَ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ قَالَ لَا ضَرَرَ وَلَا ضِرَارَ

Terjemahan: Telah menceritakan kepadaku Yahya dari Malik dari 'Amru bin Yahya Al Muzani dari Bapaknya bahwa Rasulullah Shalla Allahu 'alaihi wa sallam bersabda*: "Tidak boleh membuat kemudharatan pada diri sendiri dan membuat kemudharatan pada orang lain.". HR. Malik, No. 1234*. Hadist ini bercerita tentang bagaimana sikap dan perilaku kita terhadap diri kita sendiri dan orang lain ketika melakukan sesuatu. Pesan yang terkandung dalam hadist ini adalah untuk berhati-hati melakukan suatu perbuatan atau kegiatan yang dapat mencelakai diri kita apalagi mencelakai orang lain.

[10] Kementrian Agama Republik Indonesia, Al-Quran Dan Terjemahnya, (Bandung: Fokus media, 2010), 116.

Dari aspek perbankan, prinsip kehati-hatian dapat dilakukan melalui tindakan pencegahan oleh pihak perbankan itu sendiri. Salah satunya dengan menggunakan perangkat lunak anti *phishing* terdiri dari program komputer yang berupaya mengidentifikasi konten *phishing* yang terkandung dalam situs web dan mengirim email atau mengunci pengguna agar tidak ditipu. Ini sering diintegrasikan dengan browser web dan klien email sebagai bilah alat yang menampilkan nama domain asli untuk situs web yang dikunjungi, dalam upaya untuk mencegah situs web palsu.

Berdasarkan latar belakang diatas, maka kiranya perlu dilakukan penelitian dengan judul **"Pengaruh Prinsip Kehati-hatian Terhadap Ancaman Situs Phishing Pada Nasabah Pengguna *Internet Banking*".**

B. Rumusan Masalah

Berdasarkan latar belakang diatas, peneliti merumuskan masalah yakni: Apakah prinsip kehati-hatian berpengaruh terhadap ancaman situs *phishing* pada nasabah pengguna *internet banking*?

C. Tujuan Penelitian

Berdasarkan permasalahan di atas, maka tujuan penelitian ini yaitu untuk mengetahui seberapa besar pengaruh prinsip kehati-hatian terhadap ancaman situs *phishing* pada nasabah pengguna *internet banking*.

D. Manfaat Penelitian

1. Manfaat Teoritis

   Penelitian ini diharapkan dapat menambah pemahaman pembaca yang berkaitan dengan prinsip kehati-hatian serta menjadi sumber referensi bagi pihak yang ingin meneliti kedepannya.

2. Manfaat Praktis

   Penelitian ini diharapkan dapat digunakan sebagai acuan dan sumbangan pemikiran terhadap pemecahan masalah yang berkaitan dengan situs *Phishing.*

BAB II

KAJIAN TEORI

A. Penelitian Terdahulu yang Relevan

1. Penelitian oleh Ikhsan Radiansyah, Candiwan, dan Yudi Priyadi (2016) dalam penelitian yang berjudul "Analisis Ancaman *Phishing* Dalam Layanan *Online Banking*" dengan menggunakan metode *Systematic literature review* diperoleh hasil penelitian bahwa pengetahuan pengguna yang minim dan psikologis pengguna serta privasi social networking service pengguna adalah faktor-faktor penyebab adanya *phishing.*[1] Perbedaan dengan peneliti yaitu terletak pada variabel yang dipengaruhi, dimana penelitian ini mencari tahu penyebab *Phishing* terhadap layanan *internet banking* sementara peneliti memperhitungkan pengaruh prinsip kehati-hatian terhadap ancaman situs *Phishing* pada nasabah pengguna internet banking.
2. Aseh Ginanjar, Nur Widiyasono, dan Rohmat Gunawan (2018) dalam Penelitian yang berjudul "Analisis Serangan *Web Phishing* Pada Layanan *E-Commerce* dengan Metode *Network Forensic*". Dengan metode *network forensic process* diperoleh informasi mengenai alamat pengirim dan penerima email serta *timestamp* saat terjadi pengiriman pesan *spam* yang mengarahkan ke aktivitas *phishing*. Selain itu juga diperoleh informasi tentang *fake domain* yang terlibat

[1] Ikhsan Radiansyah, dkk, "*Analyze Phising Threats in Online Banking Service*", *Paper* (Universitas Telkom, 2016): 1.

dalam transmisi data saat terjadi aktivitas *phishing*.[12] Perbedaan dengan peneliti yaitu pada proses pengumpulan data dengan proses pengintaian secara offline dan mengumpulkan data file hasil *capture*.

3. Penelitian oleh Fadzlurrahman, Etty Mulyati, Helza Nova Lita (2020) dalam penelitian yang berjudul "Penerapan Prinsip Kehati-hatian terhadap Kepatuhan Syariah oleh Penyelenggara Teknologi Finansial". Melalui penggunaan metode deskriptif analisis yaitu menggambarkan dan menganalisis data sekunder diperoleh hasil penelitian menunjukkan bahwa kehati-hatian dalam menjalankan prinsip syariah bukan hanya menjadi tangung jawab dari penyelenggara *fintech* tetapi juga menjadi tanggung jawab dari lembaga pengawas yaitu DPS dan DSN-MUI. Perlunya dikeluarkan fatwa yang membolehkan produk-produk *fintech* yang sesuai dengan hokum syariah. Bila tidak adanya kekuatan mengikat dari fatwa maka perlu diterjemahkan ke dalam peraturan perundang-undangan dikeluarkan oleh lembaga otoritas yang berwenang.[13] Perbedaan dengan peneliti yaitu terletak pada variabel dependen yakni pada penelitian tersebut menggunakan variabel kepatuhan syariah oleh penyelenggara teknologi finansial sedangkan peneliti menggunakan

[2] Aseh Ginanjar, dkk, "Analisis Serangan Web Phising Pada Layanan E-Commerce Dengan Metode Network Forensic Process", *JUTEI* Vol 2, no. 2 (Oktober 2018): 147, https://jutei.ukdw.ac.id/index.php/jurnal/article/view/111.

[13] Fadzlurrahman, dkk, "Penerapan Prinsip Kehati-hatian terhadap Kepatuhan Syariah oleh Penyelenggara Teknologi Finansial", *Jurnal Hukum Ekonomi Syariah (J-HES)* Vol 4, no. 2 (Desember 2020): 195, https://doi.org/10.26618/j-hes.v4i02.4213.

variabel ancaman situs *Phishing* pada nasabah pengguna internet banking.

4. Yuslia Naili Rahmah (2018) dalam skripsi yang berjudul "Pengaruh Penggunaan *Internet Banking* dan Perlindungan Nasabah Pengguna Fasilitas *Internet Banking* terhadap *Cybercrime* Di Daerah Istimewa Yogyakarta (DIY)" dengan hasil penelitian yaitu terdapat pengaruh positif dan signifikan penggunaan *internet banking* terhadap *cybercrime* di Daerah Istimewa Yogyakarta, terdapat pengaruh negatif dan signifikan client charter terhadap *cybercrime* di Daerah Istimewa Yogyakarta, terdapat pengaruh positif dan signifikan kerahasiaan data nasabah terhadap *cybercrime* di daerah Istimewa Yogyakarta, tidak terdapat pengaruh dan tidak signifikan *test and trial drive* terhadap cybercrime di daerah Istimewa Yogyakarta, terdapat pengaruh positif dan signifikan consumer support service terhadap cybercrime di daerah istimewa Yogyakarta.[14] Perbedaan dari peneliti yaitu pengggunaan variabel *independent* yaitu Penggunaan *Internet Banking* dan Perlindungan Nasabah Pengguna *IB* sedangkan oleh peneliti menggunakan Prinsip Kehati-hatian pada variabel *independent*-nya.

[14] Yulia Naili Rahma, "*Pengaruh Penggunaan Internet Banking dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cybercrime Di Daerah Istimewa Yogyakarta(DIY)", Skripsi* (Universitas Negeri Yogyakarta Juni 2018): 102-103.

B. Kajian Pustaka

1. Deskripsi Teoritik

a. *Self Service Technology* (Teknologi Berbasis Layanan Mandiri)

Yang et al, (2011) menyatakan bahwa *Self Service Technology (SST)* atau teknologi berbasis layanan mandiri adalah interaksi teknologi antarmuka yang memungkinkan pelanggan untuk secara mandiri melayani diri mereka sendiri atau dapat dikatakan bahwa SST merupakan praktik melayani diri sendiri ketika membeli barang. Pelanggan semakin berusaha mengendalikan waktu dan proses dalam melakukan transaksi dan berinteraksi dengan bisnis mereka. Kemampuan untuk mengakses dan mengendalikan informasi yang mereka gunakan untuk bertransaksi khususnya melalui perbankan. Preda et al, (2008) menyatakan bahwa keuntungan utama menggunakan teknologi layanan sendiri adalah kita dapat melakukan bisnis dalam dua puluh empat jam nonstop dan mengakses mudah ke pasar global. Jadi, penggunaan teknologi berbasis layanan mandiri semakin dapat meminimumkan waktu dan biaya.

b. Enterprise Theory

Teori ini mengarah pada gagasan bahwa perusahaan berperan sebagai pranata sosial yang mana terdapat pengaruh ekonomis luas dan kompleks sehingga perlu adanya tanggung jawab sosial. Soujanen (1954) mengatakan *Enterprise theory* ini memberikan

wadah bagi pelaku perusahaan pada tahun 1950-an yang mulai memperhatikan kosumen dan masyarakat yang merupakan pusat perhatian dari pemangku kepentingan tidak langsung (*indirect*).[15]

c. Teori Anomi

Teori anomi dapat digunakan sebagai alat analisis untuk mencari penyebab orang melakukan kejahatan siber (*cybercrime*). Teori anomi beranggapan bahwa kejahatan muncul karena dalam masyarakat tidak ada norma yang mengatur suatu aktivitas tersebut (*normlesness*). Berdasarkan uraian Agus Rahardjo, dalam praktik ada sekelompok orang yang menolak kehadiran hukum untuk mengatur kegiatan di dunia maya (*virtual*). Menurut kelompok ini, dunia *virtual* adalah ruang yang bebas sehingga pemerintah tidak mempunyai kewenangan campur tangan dalam aktivitas tersebut, termasuk mengatur dengan sarana hukum. Landasan pemikiran ini diilhami oleh *Declaration of Independence of Cyberspace* dari John Perry Ballow dan Hacker Manifesto dari *Loyd Blankeship* atau *The Mentor*. Selanjutnya dijelaskan bahwa pendapat pro dan kontra tentang ada atau tidak adanya hukum yang dapat mengatur kejahatan siber (*cybercrime*) tersebut berpangkal pada kesenjangan antara karakteristik kejahatan dengan hukum pidana konvensional. Karakteristik penggunaan internet sebagai basis kegiatan bersifat

[15] Ririn Irma dariyani, "Implementasi Strategic Corporate Social Responsibility Dalam Perspektif Shari'ah Enterprise Theory", *Dinamika Global: Rebranding Keunggulan Kompetitif Berbasis Kearifan Lokal,* ISBN 978-602-60569-2-4 (2016): 846, http://jurnal.unej.ac.id/index.php/prosiding/article/download.

lintas batas sehingga sulit untuk diketahui yurisdiksinya, padahal hokum pidana konvensnional yang berlaku di Indonesia banyak yang bertumpu pada batasan-batasan tentorial. Ketentuan hukum pidana konvensional tersebut ternyata tidak dapat menyelesaikan kasus dalam aktivitas dan internet secara optimal. Namun demikian, karena saat ini sudah banyak peraturan perundang-undangan yang mengatur tentang *cybercrime*, maka sebenarnya anomi (yang diartikan sebagai ketiadaan norma secara objektif) tidak menjadi dasar rasionalitas pelaku kejahatan siber (*cybercrime*). Tetapi, jika anomi diartikan sebagai "anggapan" individu bahwa tidak ada norma (secara subjektif) tentang kejahatan siber (*cybercrime*) di Indonesia maka teori dan anggapan tersebut dapat dipahami.[16]

2. Prinsip kehati-hatian

   a. Pengertian

      Prinsip kehati-hatian atau dalam istilah bahasa inggris Prudential Principle yakni berawal dari kata "Prudent" yang berarti "Bijaksana". Istilah tersebut seringkali dikaitkan dengan fungsi pengawasan bank dan manajemen bank.

[16] Hardianto Djanggih, Nurul Qamar, "Penerapan Teori-teori Kriminologi Dalam Penanggulangan Kejahatan Siber (*Cybercrime*)", *Pandecta Vol 13 No. 1*,(2018): 20, http://dx.doi.org/10.15294/pandecta.v13i1.14020.

Menurut Abubakar dan Handayani,

> "Penerapan tata kelola yang baik pada perbankan syariah sebagai penjabaran prinsip kehati-hatian, tertumpu pada 5 pilar, yaitu: *transparency*, *accountability*, *responsibility*, *independency dan fairness"*.[17]

Istilah ini dalam perbankan digunakan untuk "asas kehati-hatian" oleh sebab itu di Negara Indonesia terbitlah istilah pengawas bank berlandaskan asas kehati-hatian, yang kemudian asas tersebut dipakai secara meluas dalam konteks yang berbeda.

Prinsip kehati-hatian (*prudent banking principle)* ialah sebuah asas yang mengungkapkan bahwasanya dalam menjalankan kegiatan usaha serta fungsinya, bank wajib bersikap hati-hati guna melindungi dana masyarakat yang diamanahkan padanya.[18] Prinsip kehati-hatian bank juga merupakan prinsip yang dalam mengoperasikan usahanya agar dalam kondisi kinerja yang baik dan memenuhi kriteria bank yang sehat.[19]

b. Landasan Prinsip Kehati-hatian

Adapun landasan penerapan prinsip kehati-hatian bank diatur dalam POJK No. 38 tahun 2016 pasal 23 ayat 3 (huruf a) yakni penyelenggaraan pemrosesan transaksi berbasis teknologi

---

[17] Lastuti Abubakar, Tri Handayani, "Telaah Yuridis terhadap Implementasi Prinsip Kehati-hatian Bank Dalam Aktivitas Perbankan Indonesia", *De Lega Lata Vol. 2 no. 1 (2017)*: 69. https://doi.org/10.31219/osf.io/acxqu.

[18] Rahma Yudi Astuti, "Penerapan Prinsip Kehati-hatian Dalam Penyaluran Pembiayaan dan Kredit Pada Lembaga Keuangan Mikro (Studi Multi Situs Pada BMT Hasanah Mlarak dan BRI Unit Mlarak, Ponorogo)", *Al Tijarah Vol. 2 no. 1 (2016)*: 31. http://ejournal.unida.gontor.ac.id/index.php/altijarah/article/download.

[19] Rosmalinda, "*Prinsip Kehati-hatian Dalam Perspektif Pencegahan Pembiayaan Mudharabah Bermasalah Di BPRS Bumi Rinjani Malang", Tesis*, (UIN Sunan Kalijaga, 2011): 31. http://digilib.uin.suka.ac.id/7017/&ved=2ahUKEwiuluDNgt3oA.

Informasi oleh pihak penyedia jasa sebagaimana dimaksud dalam ayat (2) dapat dilakukan sepanjang memenuhi prinsip kehati-hatian.[20] Selain itu prinsip kehati-hatian bagi bank berguna untuk melindungi data nasabah serta terhindar dari praktik-praktik penipuan.[21]

3. Ancaman

Menurut KBBI, ancaman menyatakan maksud (niat, rencana) untuk melakukan sesuatu yang merugikan, menyulitkan, menyusahkan, atau mencelakakan pihak lain.[22] Sebuah teori menurut Stephan dan Renfro yang dikenal sebagai *intergroup threat theory*, adalah teori dalam psikologi dan sosiologi yang mencoba menggambarkan komponen ancaman yang dirasakan yang mengarah pada prasangka antar kelompok sosial. Teori ini berlaku untuk setiap kelompok sosial yang mungkin merasa terancam, baik kelompok sosial tersebut merupakan kelompok mayoritas atau minoritas dalam masyarakat mereka atau tidak. Teori ini membahas tentang ancaman yang dirasakan daripada ancaman yang sebenarnya. Ancaman yang

[20] Asep Rozali, "Prinsip Mengenal Nasabah (Know Your Costumer Principle) Dalam Praktik Perbankan", *Jurnal Wawasan Hukum, Vol. 24 no. 1 (2011)*: 304. http://ejournal.sthb.ac.id/index.php/jwy/article/download/18.

[21] Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi Oleh Bank Umum: 23.

[22] Departemen Pendidikan Nasional, Kamus Besar Bahasa Indonesia Ed. 3, (Balai Pustaka, 2005).

dirasakan mencakup semua ancaman yang diyakini anggota kelompok mereka alami, terlepas dari apakah ancaman itu benar-benar ada.[23]

Pada tahun 2002, Stephan dan Renfro mengusulkan versi terbaru dari teori yang mereduksi empat komponen menjadi dua tipe dasar: ancaman realistis dan simbolis. Kategori stereotip negatif dan kecemasan antarkelompok telah dihapus dari kerangka dasar teori karena mereka ditemukan lebih dipahami sebagai subtipe ancaman. Mereka dapat mengarah pada ancaman yang realistis atau simbolis daripada berdiri sebagai kategori terpisah mereka sendiri. Misalnya ancaman realistis, kecemasan antarkelompok dapat didasarkan pada ekspektasi bahaya fisik. serta ancaman simbolis, ekspektasi kerusakan identitas seseorang.[24]

Berdasarkan hasil studi literatur yang telah dilakukan sebelumnya, faktor penyebab munculnya ancaman serangan phishing ketika pengguna menggunakan layanan online banking adalah minimnya pengetahuan dan psikologis pengguna. Dilihat dari pengetahuan pengguna, Zielinska, Welk, Mayhorn, & Murphy-Hill (2015) mengungkapkan:

> "Para ahli (expert) cenderung memiliki pemahaman yang lebih komprehensif tentang bagaimana tren serangan phishing dan karakteristiknya melalui e-mail dibandingkan pemula. Para ahli

[23] Walter G Stephan, Oscar Ybarra, Kimberly Rios Morrison (2009). "Intergroup Threat Theory". Dalam https://en.wikipedia.org/wiki/Integrated_threat_theory (diakses 4 September 2021).

[24] Walter G Stephan, Oscar Ybarra, Kimberly Rios Morrison (2009). "Intergroup Threat Theory". Dalam https://en.wikipedia.org/wiki/Integrated_threat_theory (diakses 4 September 2021).

dinilai lebih dapat mengambil resiko dan menghindari ancaman serangan phishing dibandingkan pengguna pemula".[25]

Selain itu dari psikologi, Vishwanath, Herath, Chen, Wang, & Rao (2011) mengungkapkan:

> "Pengguna merupakan faktor utama terjadinya penyebab phishing. Terdapat 4 alasan mengapa pengguna menjadi korban phishing. Pertama adalah semakin banyak e-mail yang diterima pengguna maka semakin besar peluang mereka ditipu. Kedua adalah pengguna umumnya akan membuka e-mail dari entitas yang mereka ketahui. Pengguna yang memiliki hubungan lebih dari satu lembaga bank dan melakukan transaksi online yang lebih banyak dibandingkan lainnya mereka berpeluang menjadi korban e-mail phishing. Yang ketiga adalah pengguna yang tidak mengetahui ancaman serangan phishing. Faktor keempat adalah kebiasaan dalam penggunaan media. Seseorang yang mempunyai kebiasaan mengecek emailnya setiap pagi sambil sarapan. Kebiasaan ini mengurangi rasa curiga dan berpeluang membuka dan mempercayai surel phishing".[26]

4. Situs *Phising*

   a. Pengertian

      Phishing adalah kata baru yang dihasilkan dari 'memancing', ini merujuk pada tindakan penyerang *indirect* yang memikat pengguna untuk mengunjungi situs Web palsu dengan mengirimi mereka email palsu (atau pesan instan), dan secara diam-diam mendapatkan informasi pribadi korban. Dalam email-email ini, mereka akan membuat beberapa penyebab, misalnya kata sandi kartu kredit Anda telah salah dimasukkan berkali-kali, atau mereka memberikan layanan peningkatan, untuk meyakinkan Anda

[25] Ikhsan Radiansyah, dkk, "*Analyze Phising Threats in Online Banking Service*", *Paper* (Universitas Telkom, 2016): 9.

[26] Ikhsan Radiansyah, dkk, "*Analyze Phising Threats in Online Banking Service*", *Paper* (Universitas Telkom, 2016): 11.

mengunjungi situs web mereka untuk menyesuaikan atau memodifikasi nomor akun Anda dan kata sandi melalui hyperlink yang disediakan dalam email.[27] Situs phising itu sendiri adalah sebuah halaman web yang dirancang oleh para cyber dengan sedemikian rupa agar menyerupai situs otentik (tampilan, konten, URL domain atau lainnya) untuk mengelabui korbannya (pengguna internet) dengan membuat korban seolah-olah sedang mengakses halaman situs dari sumber yang sah. Tampilan situs akan dibuat semirip mungkin dengan situs aslinya agar korban yakin sedang berada pada situs yang benar. Selain itu, terdapat pula situs phishing yang dirancang khusus untuk memberikan informasi atau arahan palsu yang menyesatkan. Apabila korban telah memasukkan informasi yang diminta, penjahat internet dapat dengan mudah menggunakan informasi tersebut pada situs yang sah untuk melakukan aktifitas-aktifitas yang tidak diinginkan dan tentunya hal ini akan menimbulkan kerugian yang cukup signifikan bagi para korbannya mulai dari kerugian finansial hingga *data loss*.[28] Oleh karena itu, ketika ini terjadi, peretas memiliki kesempatan untuk mendapatkan informasi pribadi dari pengguna yang

[27] E.konda Reddy, dkk, "Detecting Of E-Banking Phishing Websites", *International Journal of Modern Engineering Research (IJMER)* Vol. 2, no. 1 (2012): 46, http://www.ijmer.com/papers/vol2_issue1/I021046054.pdf.

[28] Febry Eka Purwiantono, "*Model Klasifikasi Untuk Deteksi Situs Phising Di Indonesia", Tesis*, (Institut Teknologi Sepuluh November, 2017), 1.

ditargetkan, seperti kata sandi, nama pengguna, kode keamanan, dan nomor kartu kredit, di antara hal-hal lainnya.[29]

Phisher juga bahkan dapat melanggar keamanan bank setelah mereka mengakses informasi keuangan pengguna, kemudian, mereka melakukan berbagai kegiatan illegal (mis, Menarik uang keluar dari akun Anda). Jika hal tersebut terjadi maka bank harus memperbarui langkah-langkah keamanan mereka secara teratur dan memastikan bahwa transaksi antara mereka dan pelanggan mereka aman. Bank harus menggunakan beberapa jenis tindakan balasan yang diperbarui, seperti otentikasi dua faktor, bersama dengan program perangkat lunak perlindungan lainnya. [30]

Janji e-bank dalam menurunkan biaya transaksi dan mampu menjangkau massa dapat dan hanya akan terwujud ketika pengguna mempercayai sistem transaksi online dan risiko transaksi dikurangi jika tidak dihapus. Phishing adalah penyebab utama dalam erosi kepercayaan pengguna terhadap transaksi perbankan Internet.[31] Sejumlah penelitian baru-baru ini mencoba menjelaskan bagaimana dan mengapa orang menjadi korban kejahatan ini.

---

[29] V. Suganya, "A Review on Phishing Attacks and Various Anti Phishing Techniques", *International Journal of Computer Applications* Vol. 139, no. 1 (2016): 23, https://www.ijcaonline.org/archives/volume139/number1/24454-2016909084.

[30] Alhussan O. Al syed, Anwar L. Bilgrami, "E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities", *International Journal of Emerging Technology and Advanced Engineering* Vol 7, no. 1 (2017): 114, http://www.cybercrimejournal.com/Jansen&Leukfeldtvol10issue1IJCC2016.

[31] Gerald Goh Guan Gan, "Phishing: A Growing Challenge for Internet Banking Providers in Malaysia", *Communications of the IBIMA* Vol. 5, (2008): 140, http://ibimapublishing.com/articles/CIBIMA/2008/252213/252213.

Leukfeldt (2015), melakukan studi eksplorasi tentang bagaimana pelanggan menjadi korban penipuan perbankan online dan menunjukkan bahwa pelanggan memiliki peran spesifik dalam viktimisasi mereka sendiri. Pelanggan memberikan informasi kepada penipu, seperti kredensial, yang dapat digunakan penipu untuk mencuri uang dari rekening bank mereka. Sebuah studi tentang *phishing* viktimisasi menunjukkan bahwa semua orang berisiko menghadapi kejahatan jenis ini.[32]

Phishing adalah sebuah aktifitas kriminal dalam mencuri informasi pribadi yang sifatnya sensitif seperti username dan password melalui penyamaran sebagai entitas yang terpercaya dan membuat korban tidak sadar telah memberikan informasi sensitif ke *scammer*.[33] Pada tahun 1995, phising mulai terkenal di dunia cybercrime. Phishing pun juga sering disebut sebagai brand spoofing atau carding yaitu sebuah layanan web untuk mengelabui anda dengan menjanjikan keamanan transfer beserta keabsahan data yang anda lakukan.[34] APWG mengirimkan hasil yang menyatakan bahwa terjadi serangan phishing sebesar 263.538 kasus pada kuartal pertama tahun 2018 lalu. Dan perlu diketahui

[32] Jurjen Jansen dan Rutger Leukfeldt, "Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization", *International Journal of Cyber Criminology* Vol. 10, no. 1 (2016): 80, http://www.cybercrimejournal.com/Jansen&Leukfeldtvol10issue1IJCC2016.

[33] Ikhsan Radiansyah, dkk, "*Analyze Phising Threats in Online Banking Service*", *Paper* (Universitas Telkom, 2016): 5.

[34] Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber", *Jurnal SAINTIKOM* Vol. 13, no. 3 (September 2014): 211, https://prpm.trigunadharma.ac.id/public/fileJurnal/hpG3Jurnal%20Dian%20Rahmawaty2014.

bahwa sebenarnya telah terjadi peningkatan serangan phishing sekitar 46% kasus pada kuartal keempat tahun 2017 silam, dimana sektor e-commerce menjadi target utama dari 32,4% dari jumlah kasus yang terjadi.[35]

Adapun kasus yang terkenal berkenan dengan hal ini adalah kasus website Bank Central Asia (BCA) yang pernah terjadi di tahun 2001. Dimana pada layanan internet banking (BCA) menggunakan sebuah URL yang berbeda namun tetap memiliki persamaan dalam hal penyebutan maupun kesalahan ketik. Adapun cara kerja Phishing adalah ketika seseorang menginput username beserta passwordnya pada halaman login palsu, maka data tersebut akan terekam dan terkirim pada admin dari login palsu tersebut.[36] Dan kembali terjadi lagi pada tahun 2015 pada Bank Mandiri oleh Nasabah di Bengkulu dimana terdapat rekening nasabah atas nama Firdaus akan melakukan transfer ke rekening BTN Cabang Nusa Dua Bali atas nama Risto Matilah sebesar Rp. 49.157.889. Dalam riwayat transaksi dinyatakan berhasil, namun sebenarnya transaksi tersebut telah diambil alih oleh *hacker*. Hal serupa juga terjadi pada nasabah Seprinaldi yang akan melakukan transfer ke rekening bank Sinarmas. Pihak bank beranggapan bahwa nasabah tersebut telah menjadi korban penipuan dengan modus sinkronisasi token

[35] Aseh Ginanjar, dkk, "Analisis Serangan Web Phising Pada Layanan E-Commerce Dengan Metode Network Forensic Process", *JUTEI* Vol 2, no. 2 (Oktober 2018): 147, https://jutei.ukdw.ac.id/index.php/jurnal/article/view/111.

[36] Vyctoria, *Bongkar Rahasia E-Banking Security Dengan Teknik Hacking dan Carding*,Ed. 1, (Yogyakarta : *Andi* Offset, 2013), 213.

pada saat membuka laman internet banking menggunakan komputer pribadi korban yang telah berisi virus dan bukan berasal dari bank Mandiri.[37]

b. Ada beberapa hal yang perlu dicermati agar terhindar dari serangan *phising*:[38]

1) Telusuri latar belakang email yang diterima. Biasanya, si penyerang menggunakan modus mengirimkan email pancingan ke sejumlah calon korban. Biasanya berisi perintah untuk melakukan login di sebuah website palsu, dengan mengisi kolom registrasi ulang dan menginput username beserta password e-banking nasabah.
2) Menghubungi *customer service* bank. Untuk memverifikasi tentang kebenaran prosedur registrasi password ulang akan sangat berguna jika kita menghubungi customer service bank.
3) Perbedaan website yang asli dengan tiruan. Suatu bank menggunakan protokol Hyper Text Transfer Protocol Secure (https) pada websitenya.

c. *Cyber crime* yang dilakukan oleh seorang *phiser* menggunakan beberapa teknik *Phising* antara lain:[39]

1) Email Spoofing

[37] Republika.co.id, "*Rekening Pelaku Phising Nasabah Mandiri Bengkulu Dibekukan*" *https://republika.co.id/berita/nsuvn6257/rekening-pelaku-emphisingem-nasabah-mandiri-bengkulu-dibekukan* (diakses 21 Januari 2020).

[38] Rifqy Hakimi, "Studi Isu Keamanan Jaringan Pada Facebook", *Jurnal Pustakawan Indonesia Vol*. 11, no. 2 (2012): 8, https://journal.ipb.ac.id/index.php/jpi/article/view/11421.

[39] Aseh Ginanjar, dkk, "Analisis Serangan Web Phising Pada Layanan E-Commerce Dengan Metode Network Forensic Process", *JUTEI* Vol 2, no. 2 (Oktober 2018): 148, https://jutei.ukdw.ac.id/index.php/jurnal/article/view/111.

Teknik ini biasa digunakan *phiser* dengan cara mengirim email secara *broadcast* ke jutaan pengguna, seolah-olah berasal dari institusi resmi yang berisi seruan untuk melakukan sesuatu. Biasanya e-mail berisi pemintaan nomor kredit, password atau mengunggah form tertentu.

2) *Pengiriman* Berbasis Web

Pengiriman Berbasis Web adalah salah satu teknik phishing yang dikenal sebagai "man-in-the-middle", phiser terletak diantara situs web asli dan sistem phishing.

3) *Pesan* Instan (*chatting*)

Olah pesan cepat adalah metode dimana pengguna menerima pesan berupa link yang diarahkan ke situs web palsu yang memiliki tampilan sama sehingga pengguna merasa mengakses situs web resmi yang sah padahal palsu.

4) *Trojan* hosts

Trojan *hosts, phiser* mencoba *login* ke *account* pengguna untuk mengumpulkan kredensial melalui mesin lokal. Informasi yang diperoleh kemudian dikirim ke *phisher*.

5) Manipulasi *tautan* (*link*)

Manipulasi *link* adalah teknik dimana *phisher* mengirimkan *link* ke sebuah *website*. Bila pengguna melakukan *click* pada *link* tersebut, maka akan diarahkan ke *website phisher* yang bukan *link website* sebenarnya.

6) Malware Phishing

Penipuan yang melibatkan malware untuk dijalankan pada komputer pengguna. Malware ini biasanya melekat pada e-mail yang dikirimkan kepada pengguna oleh *phisher*. Setelah korban melakukan klik pada link, maka malware akan mulai berfungsi. Malware tersebut terkadang disertakan pada file yang dapat download.

7) *Dropbox Phishing*

Seperti jutaan dari orang menggunakan *Dropbox* setiap hari untuk cadangan, akses dan berbagi file mereka. Oleh karena itu, para penyerang akan mencoba untuk memanfaatkan pada popularitas platform dengan menargetkan pengguna dengan email *phishing*. Satu kampanye serangan, untuk misalnya, mencoba untuk memancing pengguna agar memasukkan kredensial login mereka pada palsu *Dropbox* masuk halaman host di *Dropbox* itu sendiri.[40]

d. Hasil analisis identifikasi menunjukkan bahwa *hyperlink phishing* memiliki satu atau beberapa karakteristik diantaranya:[41]

1) Tautan visual dan tautan sebenarnya tidak sama

[40] Deepashree K. Mehendale, et al., "Review of Phishing attacks and Anti Phishing Tools", *International Journal Of Innovative Research In Computer And Communication Engineering (IJRCCE)* Vol. 5, no. 9 (2017): 15132, http://www.ijircce.com/upload/2017/september/49_Final_Paper%20_16_.

[41] E.konda Reddy, et al., "Detection Of E-Banking Phishing Websites", *International Journal of Modern Engineering Research (IJMER)* Vol. 2, no. 1 (2012): 46, http://www.ijmer.com/papers/vol2_issue1/I021046054.

2) Penyerang sering menggunakan alamat IP desimal bertitik bukannya nama DNS
3) Trik khusus digunakan untuk menyandikan hyperlink dengan jahat;
4) Penyerang sering menggunakan nama DNS palsu yang mirip (tetapi tidak identik) dengan situs Web target .

Kami kemudian mengusulkan algoritma anti-*phishing* berbasis host akhir yang kami sebut *Link Guard*, berdasarkan karakteristik *hyperlink phishing*. Karena *Link Guard* berbasis karakter, ia dapat mendeteksi dan mencegah tidak hanya serangan *phising* yang diketahui tetapi juga yang tidak dikenal. Kami telah menerapkan *Link Guard* di Windows XP, dan percobaan kami menunjukkan bahwa *Link Guard* berbobot ringan karena mengkonsumsi sangat sedikit memori dan lingkaran CPU, dan yang paling penting, sangat efektif dalam mendeteksi serangan phishing dengan negatif palsu minimal.

5. Internet Banking

a. Pengertian

Internet merupakan jaringan yang menyediakan sambungan menuju global informasi yang terdiri dari sekumpulan jaringan yang terhubung antara satu dengan lainnya. Sedangkan *internet banking* merupakan suatu pelayanan bank dalam mempromosikan produk serta bertransaksi dengan memanfaatkan media internet

secara online. Efisiensi penyelenggaraan kegiatan usaha bank meningkat dengan kehadiran internet banking. Internet Banking merupakan salah satu produk jasa pelayanan Bank yang disediakan untuk nasabah agar lebih mudah mengakses internet atau melakukan transaksi keuangan, transfer, bisnis, maupun informasi lainnya yang dapat diakses melalui jaringan internet. Internet banking tidak hanya memberikan kenyamanan namun juga kemudahan karena menu-menu pada internet banking dapat digunakan tanpa harus memiliki keterampilan khusus. Serta aman karena internet banking dilengkapi dengan sistem keamanan berlapis dan dilengkapi dengan token atau (alat yang mengeluarkan angka-angka password yang selalu berganti setiap kali saat melakukan transaksi keuangan). Disisi lain e-banking merupakan layanan yang memungkinkan nasabah bank untuk memperoleh informasi, melakukan komunikasi, dan melakukan transaksi perbankan melalui media elektronik. Sementara itu volume Transaksi perbankan dengan menggunakan internet banking di Indonesia baik secara frekuensi maupun volume terus mengalami peningkatan. Pada tahun 2014, volume internet banking sudah mencapai Rp. 6.447 triliun atau naik 17,32% di bandingkan dengan tahun sebelumnya. ternyata pengguna internet banking juga didominasi oleh usia muda. Hal ini dapat kita lihat dari hasil survey yang dilakukan oleh Penyelenggara Jasa Internet Indonesia

(APJII). Dari survey tersebut diketahui, bahwa 49,52% pengguna internet banking berusia 19 - 34 tahun, kemudian 29,55% berusia 35-54 tahun, dan 4,24% berusia 54 tahun keatas.[42]

Terdapat tiga tahap pelayanan internet banking yang ditawarkan kepada nasabah, yaitu layanan informasi (*informational*) dimana bank hanya menyediakan informasi jasa keuangan dalam websitenya, komunikasi (*communicational*) dimana dalam website tersebut juga memungkinkan nasabah untuk dapat berkomunikasi dengan bank, transaksi (*transacttional/advance*) dimana sudah memungkinkan nasabah untuk melakukan transaksi-transaksi keuangan virtual seperti, transfer dana, pengecekan saldo, ataupun jenis pembayaran.[43]

Pengertian *Internet Banking* menurut Budi Agus Riswandi merupakan salah satu layanan jasa Bank yang memungkinkan nasabah untuk menerima informasi, melakukan komunikasi serta transaksi perbankan melalui media internet.[44] Definisi *internet banking* menurut Cronin (1998) adalah "*the financial services application that enables financial institutions to offer traditional banking products and services such as checking, savings and*

[42] Rosmida Murfi, Teguh Suripto, "Analisa Minat Mahasiswa Terhadap Penggunaan Layanan Internet Banking Bank BNI Syariah", *Jurnal Ekonomi Syariah Indonesia* Vol. X, No. 1 (2020): 58, https://ejournal.almaata.ac.id/index.php/JESI/article/view/1349/1337.

[43] Lydia Arie Widyarini, "Analisis Niat Perilaku Menggunakan Internet Banking Di Kalangan Pengguna Internet Di Surabaya", *Jurnal Widya Manajemen & Akuntansi* Vol 5, No. 1 (Surabaya April 2005): 109-110, http://journal.wima.ac.id/index.php/JWMA/article/view/1177.

[44] H. Djohar Arifin, "Pengaruh Internet Banking Terhadap Tingkat Kepercayaan Nasabah Pada Bank Bri Syariah Kcp Arjawinangun", *Al-Amwal* Vol 8, No. 2 (Cirebon 2016): 533, https://syekhnurjati.ac.id/jurnal/index.php/amwal/article/view/1610.

money accounts and certificates of deposit over internet". Kegiatan perbankan yang dilakukan secara online dalam hal ini adalah internet banking sifatnya lebih fleksibel karena tidak dibatasi ruang dan waktu, sehingga nasabah dapat menjangkau layanan dari manapun dan kapanpun.

Menurut Atorf, et al., (2002), *internet banking* dibedakan dalam 3 tingkatan, yaitu:[45]

1) *Entry informational*

   Yaitu menyediakan informasi statistik mengenai bank tersebut serta jasa/ produk yang ditawarkan melalui brosur elektronik dari suatu bank. Karena tahapan ini sangat sederhana maka risikonya sangat rendah karena tidak terhubung dengan data base bank.

2) *Intermediate/ communicative*

   Dimana nasabah dapat melakukan interaksi dengan bank penyedia jasa internet secara terbatas, misalnya *account inquiry*, *online account application*, *electronic mail*, dan sebagainya. Karena pelayanannya lebih luas daripada sekedar informasi maka tahap ini memiliki risiko yang lebih besar.

3) *Advance/ transaction*

   Dimana seluruh transaksi yang diperlukan oleh nasabah termasuk transfer dana, pembayaran tagihan dan lain-lain

[45] Lydia Arie Widyarini, "Analisis Niat Perilaku Menggunakan Internet Banking Di Kalangan Pengguna Internet Di Surabaya", *Jurnal Widya Manajemen & Akuntansi* Vol 5, No. 1, (Surabaya April 2005): 109-110, http://journal.wima.ac.id/index.php/JWMA/article/view/1177.

layaknya pelayanan melalui counter atau ATM kecuali penarikan kas ditampilkan. Oleh sebab itu tahapan ini adalah yang paling lengkap.

Sedangkan menurut Furs et al. mendefinisikan *Internet Banking* sebagai saluran perpanjangan jarak jauh untuk mengantarkan jasa-jasa perbankan. Adapun jasa-jasa perbankan yang diberikan *internet banking* yaitu seperti pembukaan rekening tabungan, melakukan transfer dana antar rekening, serta tagihan pembayaran elektronik. Selain itu, Karen Frust mengemukakan bahwa terdapat dua jenis perbankan melalui *Internet Banking*. Pertama, bank yang memiliki bangunan kantor cabang dapat membuat situs internet dan menawarkan layanan perbankan yang diberikan melalui kantor cabangnya. Kedua, bank yang hanya memberikan jasa layanan perbankan melalui internet banking atau bank tanpa Kantor Cabang (branchless) biasa juga disebut virtual bank dan *internet only bank*.[46]

b. Produk atau Jasa Internet Banking

Melalui internet banking terdapat jenis produk/jasa yang ditawarkan:[47]

[46] H. Djohar Arifin, "Pengaruh Internet Banking Terhadap Tingkat Kepercayaan Nasabah Pada Bank Bri Syariah Kcp Arjawinangun", *Al-Amwal*, Vol 8, No. 2 (Cirebon 2016): 533, https://syekhnurjati.ac.id/jurnal/index.php/amwal/article/view/1610.

[47] Yulia Naili Rahma, *"Pengaruh Penggunaan Internet Banking dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cybercrime Di Daerah Istimewa Yogyakarta(DIY)", Skripsi* (Universitas Negeri Yogyakarta Juni 2018), 29-30.

1) Informasi saldo
2) Pembukaan rekening
3) Transfer, dimana cara ini adalah yang paling efisien dan murah karena nasabah dapat melakukannya dimana saja tanpa dibatasi oleh waktu.
4) *Payment Gateway*, merupakan fasilitas disediakan oleh bank untuk nasabah yang ingin melakukan pembayaran telepon, air PAM, dan listrik langsung melalui internet.

   Konsep *payment gateway* ini mirip dengan transfer karena nasabah maupun penyedia jasa (perusahaan telepon atau listrik) harus sama-sama memiliki account di bank tersebut.[48]
5) *Kliring* , Secara Umum diuraikan sebagai transaksi yang aktivitasnya dijadikan sebagai lalu lintas pembayaran yang dimana kesepakatan terjadi antar bank dengan menyertakan Data Keuangan berupa data Elektronik yang dilakukan dalam jangka pendek. Dalam menjalankan kegiatan kliring perlu adanya penyelenggaraan sistem yang terdiri dari 2 jenis yakni secara sistem manual dan sistem otomatis. Penyelengara SKNBI, Sistem Kliring Nasional Bank Indonesia dilakukan Penyelenggara Kliring Nasional, mempunyai tugas melaksanakan SKNBI nasional. Penyelenggara Kliring Lokal,

[48] Ioannis V. Koskosas, "Trust and Risk Communication in Setting Internet Banking Security Goals", *Risk Management* Vol 10, No. 1 (Greece Februari 2008): 59-60, https://www.researchgate.net/publication/32042765_Trust_and_Risk_Communication_in_Setting_Internet_Banking_Security_Goals.

adalah bagian dari Bank Indonesia yang melaksanakan SKNBI di daerah kliring tertentu. Dalam penyelenggaraannya tentunya pihak bank perlu adanya peserta kliring yang dalam hal ini ada dua yaitu Peserta langsung, adalah semua bank yang terdaftar bisa mengira notanya langsung dengan BI. Dan Peserta tidak langsung, adalah semua bank yang tidak tercantum sebagai peserta tetapi mengikuti kegiatan kliring memalui bank yang telah terdaftar. Berdasarkan jenisnya kliring dibagi menjadi tiga yakni Kliring umum, merupakan perhitungan warkat dilaksanakan dan diatur oleh BI. Kliring lokal, perhitungan warkat yang terletak di wilayah kliring. Kliring antar cabang, perhitungan warkat antar kantor cabang peserta diwilayah yang sama.[49]

6) *Trade Finance and Services*, menandakan pembiayaan untuk perdagangan, dan itu menyangkut transaksi perdagangan domestik dan internasional. Transaksi perdagangan membutuhkan penjual barang dan jasa serta pembeli. Berbagai perantara seperti bank dan lembaga keuangan dapat memfasilitasi transaksi ini dengan membiayai perdagangan.
7) *Penutupan* rekening
8) *Transaksi* lainnya

[49] Cherry Agustine Chandra, I Gede Suwetja, "Ipteks Peran BI Terhadap Transfer Dana Melalui Sistem Kliring Nasional PT. Bank Sulutgo", *Jurnal Ipteks Akuntansi bagi Masyarakat* Vol 2, No. 2 (2018): 643-644, https://media.neliti.com/media/publications/294269-ipteks-peran-bi-terhadap-transfer-dana-m-e08358af.

Adapun fasilitas lain yang ada pada internet banking dapat melakukan berbagai transaksi, di antaranya:[50]

1) Melihat transaksi terakhir
2) Melihat atau mendownload laporan bank atau mutasi
3) Transfer ke bank lain, baik secara RTGS maupun LLG. LLG (Lalu Lintas Giro) adalah mekanisme transfer antarbank dengan menggunakan fasilitas kliring, sedangkan RTGS (*Real Time Goss Settlement*) adalah mekanisme transfer antarbank secara *real time.*
4) Membayar pihak ketiga, termasuk pembayaran tagihan
5) Pembelian voucher pulsa, reksa dana, tiket pesawat, dan sebagainya.

Masih banyak lagi transaksi lain yang bisa dilakukan, tergantung fasilitas yang diberikan oleh pihak bank. Biasanya aktivitas internet banking yang dilakukan melalui *web browser* dengan menggunakan SSL yang aman.

c. Sistem Keamanan Internet Banking[51]

Sistem keamanan bertransaksi perbankan dengan menggunakan internet menjadi salah satu isu yang menjadi permasalahan dalam penggunaan internet banking. Adapun masalah yang kerap terjadi adalah adanya pencurian nomor kartu kredit. Orang yang tidak

[50] Vyctoria, *Bongkar Rahasia E-Banking Security Dengan Teknik Hacking dan Carding* Ed.1, (Yogyakarta : Andi Offset, 2013), 71.

[51] Yulia Naili Rahma, "*Pengaruh Penggunaan Internet Banking dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cybercrime Di Daerah Istimewa Yogyakarta(DIY)", Skripsi* (Universitas Negeri Yogyakarta Juni 2018), 31-32.

bertanggung jawab tersebut mengambil kesempatan untuk memanfaatkan nomor kartu kredit hasil curiannya. Pihak bank harus meyakinkan nasabah bahwa transaksi perbankan berjalan aman karena bank bersangkutan memiliki perangkat keamanan untuk mencegah para *hacker* mengganggu transaksi mereka.

Ada dua jenis sistem keamanan yang dipakai dalam internet banking yaitu :

1) Sistem *Cryptography*

Kriptografi adalah ilmu dan teknik dalam pengamanan data dari pihak ketiga. Sistem ini menggunakan angka-angka yang dikenal dengan sistem sandi. Pada kriptografi terdapat istilah enkripsi dan dekripsi. Enkripsi adalah mengubah text awal (*plain text*) menjadi text ter-enkripsi (*cipher text*) menggunakan sebuah kunci.[52] Sedangkan Dekripsi adalah mengubah text ter-enkripsi (*cipher text*) kembali menjadi text awal (*plain text*) dengan menggunakan kunci yang sama, dalam hal ini jika menggunakan *symmetric-key cryptography*.

Tipe *cryptography* terdapat tiga macam, diantaranya:[53]

a) Kriptografi Kunci Simetris (*Symmetric Key Cryptography*)

[52] Angga Aditya Permana, Desi Nurnaningsih, "Application of Cryptography With Data Encryption Standard (DES) Algorithm in Picture", *JIKA (Jurnal Informatika)*, Vol 4, No. 2 (2020): 83, http://jurnal.umt.ac.id/index.php/jika/article/view/2640/1762.

[53] Angga Aditya Permana, Desi Nurnaningsih, "Application of Cryptography With Data Encryption Standard (DES) Algorithm in Picture", *JIKA (Jurnal Informatika)*, Vol 4, No. 2 (2020): 83, http://jurnal.umt.ac.id/index.php/jika/article/view/2640/1762.

Kriptografi ini menggunakan kunci yang sama untuk enkripsi dan dekripsi pesan. Dimana pengirim dan penerima pesan menggunakan kunci yang sama untuk enkripsi dan dekripsi pesan dan hal ini memungkinkan seseorang untuk mengganggu ditengah jalan. Ada beberapa macam algoritma yang termasuk ke dalam *symmetric-key cryptography*, salah satu algoritma yang paling terkenal dari Kriptografi kunci simetris ini adalah DES (Data Encryption Standard).

b) Kriptografi Kunci Asimetris (*Asymmetric Key Cryptography*)

Kriptografi ini menggunakan sepasang kunci yang berbeda untuk enkripsi dan dekripsinya. Biasanya digunakan untuk mengenali nasabah dan melindungi informasi finansial nasabah sehingga jumlah kecepatan pengiriman data menjadi berkurang karena adanya tambahan kode. Sebuah kunci publik (*public key*) digunakan untuk enkripsi dan kunci rahasia (*private key*) digunakan untuk dekripsi. P*ublic key* dan *Private Key* adalah hal yang berbeda. Walaupun jika kunci publik diketahui oleh semua orang, hanya penerima lah yang dapat men-

decrypt informasi tersebut karena hanya dia yang tahu kunci rahasia (*private key*) nya.

c) Kriptografi *Hybrid*

Kriptografi ini memadukan *symmetric* dan *asymmetric cipher* dalam penggunaannya. Pengirim mengenkripsi pesan dengan *session key*, lalu *session key* tersebut di-*encrypt* kembali dengan menggunakan *public key*. Lalu, penerima men-*decrypt session key* tersebut dengan *priate key* yang dimilikinya.

2) Sistem *Firewall*

Dalam dunia nyata, Firewall adalah dinding yang bisa memisahkan ruangan, sehingga kebakaran pada suatu ruangan tidak menjalar ke ruangan lainnya. Tapi sebenarnya *firewall* diinternet lebih seperti pertahanan disekeliling benteng, yakni mempertahankan terhadap serangan dari luar. Sistem ini berguna untuk membatasi gerak orang yang masuk ke dalam jaringan internal, membatasi gerak orang yang keluar dari jaringan internal, serta mencegah penyerang mendekati pertahanan yang berlapis.[54] *Firewall* dapat mencegah pihak-pihak yang tidak diizinkan untuk mencoba masuk tanpa izin dengan cara melipatgandakan dan mempersulit hambatan-

[54] Fajar Adhi Purwaningrum, dkk, "Optimalisasi Jaringan Menggunakan Firewall", *Jurnal IKRA - ITH Informatika*, Vol 2, No. 3 (2018): 19, https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/download/251/144.

hambatan yang ada atau dengan kata lain tidak diizinkan untuk memasuki daerah yang dilindungi dalam unit pusat kerja perusahaan. Namun, hal yang digaris bawahi adalah sistem *firewall* ini tidak dapat mencegah masuknya virus atau gangguan yang berasal dari dalam perusahaan itu sendiri.

Tipe *firewall* terdapat empat macam, diantaranya:[55]

a) Packet *Filtering Router*

Firewall jenis ini memfilter paket data berdasarkan alamat dan pilihan yang sudah ditentukan terhadap paket tersebut. Ia bekerja dalam level internet protocol (IP) paket data dan membuat keputusan mengenai tindakan selanjutnya (diteruskan atau tidak diteruskan) berdasarkan kondisi dari paket tersebut.

b) Circuit *Gateways*

Firewall jenis ini beroperasi pada layer (lapisan) transport pada network, dimana koneksi juga diautorisasi berdasarkan alamat. Sebagaimana halnya Packet Filtering, Circuit Gateway (biasanya) tidak dapat memonitor trafik data yang mengalir antara satu network dengan network lainnya, tetapi ia mencegah koneksi langsung antar network.

c) Application *Gateways*

[55] Fajar Adhi Purwaningrum, dkk, "Optimalisasi Jaringan Menggunakan Firewall", *Jurnal IKRA - ITH Informatika*, Vol 2, No. 3 (2018): 19, https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/download/251/144.

Firewall tipe ini juga disebut sebagai firewall berbasis proxy. Ia beroperasi dilevel aplikasi dan dapat mempelajari informasi pada level data aplikasi (yang dimaksudkan disini adalah isi (content) dari paket data karena proxy pada dasarnya tidak beroperasi pada paket data). Filterisasi dilakukan berdasarkan data aplikasi, seperti perintahperintah FTP atau URL yang diakses lewat HTTP. Dapat dikatakan bahwa firewall jenis ini "memecah model clientserver".

d) Hybrid *Firewall*

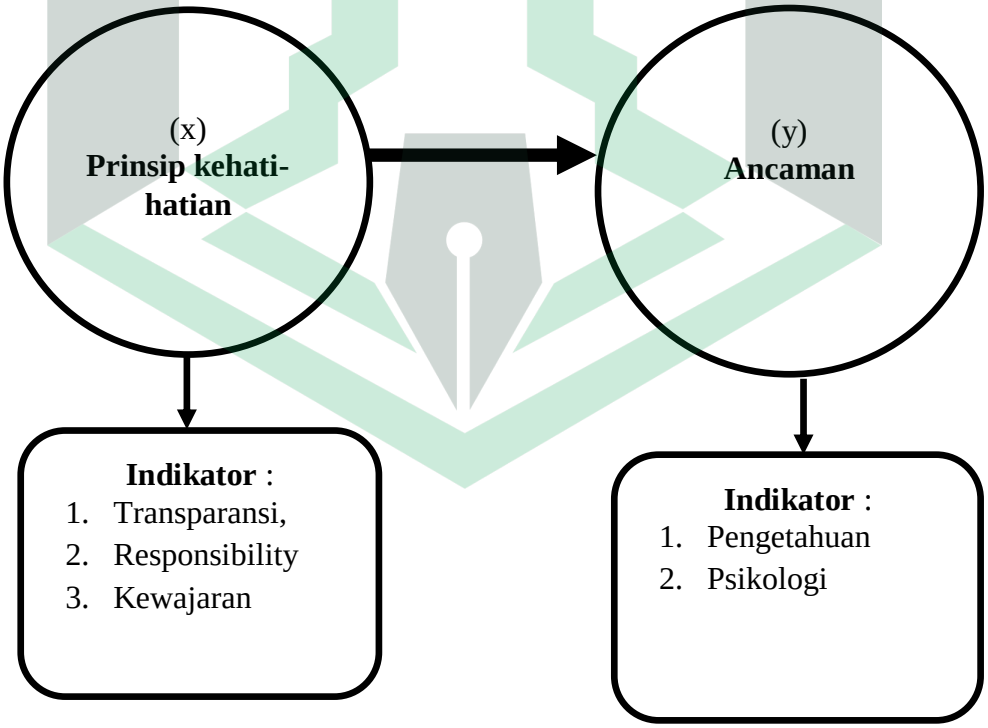
Firewall jenis ini menggunakan elemen-elemen dari satu atau lebih tipe firewall. Hybrid firewall sebenarnya bukan sesuatu yang baru. Firewall komersial yang pertama, DECSEAL, adalah firewall berjenis hybrid, dengan menggunakan proxy pada sebuah bastion hosts (mesin yang dilabeli sebagai "gate keeper") dan packet filtering pada gateway ("gate"). Sistem hybrid sering kali digunakan untuk menambahkan layanan baru secara cepat pada sistem firewall yang sudah tersedia. Kita bisa saja menambahkan sebuah circuit gateway atau packet filtering pada firewall berjenis application gateway, karena untuk itu hanya diperlukan kode proxy yang baru yang ditulis untuk setiap service baru yang

akan disediakan. Kita juga dapat memberikan autentifikasi pengguna yang lebih ketat pada *Stateful Packet Filer* dengan menambahkan proxy untuk tiap service.

C. Kerangka Pikir

Penelitian ini menggunakan regresi linier sederhana dengan variabel bebas yaitu Prinsip Kehati-hatian dan faktor yang dipengaruhinya yaitu Ancaman Situs *Phishing* pada nasabah pengguna internet banking.

"Pengaruh Prinsip Kehati-hatian terhadap Ancaman Situs *Phishing* Pada Nasabah Pengguna Internet Banking"



Gambar 2.1 Skema Kerangka Pikir

D. Hipotesis

Berdasarkan landasan teori yang didukung dengan penelitian terdahulu serta rumusan masalah yang ada, maka hipotesis dapat dirumuskan sebagai berikut :

Ha : Terdapat pengaruh prinsip kehati-hatian terhadap ancaman situs *phishing* pada nasabah pengguna *internet banking*

Ho : Tidak terdapat pengaruh prinsip kehati-hatian terhadap ancaman situs *phishing* pada nasabah pengguna *internet banking*

BAB III

METODE PENELITIAN

A. Jenis Penelitian

Jenis penelitian yang digunakan adalah penelitian kuantitatif. Menurut Sugiyono, metode penelitian kuantitatif dapat diartikan sebagai metode yang digunakan untuk meneliti populasi dan sampel tertentu dengan teknik pengambilan sampel umumnya secara random, kemudian pengumpulan data menggunakan instrumen penelitian yang bertujuan untuk menguji hipotesis yang telah ditetapkan dengan berlandaskan pada filsafat *positivisme*.[56] Penelitian ini juga digunakan untuk menghitung seberapa besar pengaruh variabel x terhadap variabel y.

B. Lokasi dan Waktu Penelitian

Lokasi penelitian merupakan suatu wilayah atau daerah tempat peneliti melakukan proses penelitian untuk mendapatkan data-data terkait yang di butuhkan. Yang dimana penelitian ini di lakukan di Bank Syariah Mandiri Palopo, BRI Syariah Palopo dan BNI Syariah Palopo, Sulawesi Selatan. Dan waktu penelitian ini dilakukan pada Tanggal 17 Juni s/d 17 Agustus 2020.

[56] Sugiyono, *Metode Penelitian Bisnis (Pendekatan Kuantitatif, Kualitatif*, dan R&D), (Bandung: CV Alfabeta, 2013), 13.

C. Definisi Operasional Variabel

Pada penelitian ini untuk memahami arah dari pembahasan judul maka perlu dideskripsikan dengan jelas dalam tebel berikut.

Tabel 3.1

Definisi Operasional Variabel

No.	Variabel	Definisi	Indikator
1	Prinsip kehati-hatian (X)	Prinsip kehati-hatian (*prudent banking principle)* ialah sebuah asas yang mengungkapkan bahwasanya dalam menjalankan kegiatan usaha serta fungsinya, bank wajib bersikap hati-hati guna melindungi dana masyarakat yang diamanahkan padanya.[57]	Transparansi, Responsibility, Kewajaran[58]

[57] Rahma Yudi Astuti, "Penerapan Prinsip Kehati-hatian Dalam Penyaluran Pembiayaan dan Kredit Pada Lembaga Keuangan Mikro (Studi Multi Situs Pada BMT Hasanah Mlarak dan BRI Unit Mlarak, Ponorogo)", *Al Tijarah Vol. 2 no. 1 (2016)*: 31. http://ejournal.unida.gontor.ac.id/index.php/altijarah/article/download.

[58] Lastuti Abubakar, Tri Handayani, "Telaah Yuridis terhadap Implementasi Prinsip Kehati-hatian Bank Dalam Aktivitas Perbankan Indonesia", *De Lega Lata Vol. 2 no. 1 (2017)*: 69. https://doi.org/10.31219/osf.io/acxqu.

2	Ancaman (Y)	Ancaman pada sistem komunikasi data atau jaringan komputer adalah penghancuran informasi, perubahan/modifikasi data, pencurian informasi data, pangungkapan informasi serta penghentian layanan.[59]	Pengetahuan, Psikologi[60]

D. Populasi dan Sampel

Menurut Sugiyono, mengartikan populasi sebagai wilayah generalisasi yang terdiri atas obyek/subyek yang mempunyai kualitas dan karakteristik tertentu yang ditetapkan oleh peneliti untuk dipelajari dan kemudian ditarik kesimpulannya.[61] Populasi juga dapat di definisikan sebagai seperangkat unit analisis yang lengkap yang sedang diteliti.[62] Populasi dalam penelitian ini adalah nasabah pengguna internet banking.

Sementara itu, sampel merupakan bagian dari populasi yang akan diteliti. Oleh karena itu sampel harus dilihat sebagai suatu pendugaan

[59] Yudhi Kusnanto, "Analisis Kerentanan Dan Kehandalan Layanan Jaringan Cloud Berbasis Platform Eucalyptus", *Jurnal Sistem Informasi (JSI)* Vol. 8, no. 1 (2016): 46. http://ejournal.unsri.ac.id/index.php/jsi/index.

[60] Ikhsan Radiansyah, dkk, "*Analyze Phising Threats in Online Banking Service*", *Paper* (Universitas Telkom, 2016): 9.

[61] Sugiyono, *Metode Penelitian Bisnis (Pendekatan Kuantitatif, Kualitatif*, dan R&D), (Bandung: CV Alfabeta, 2013), 389.

[62] Jonathan Sarwono, *Metode Penelitian Kuantitatif dan Kualitatif*, (Yogyakarta: Graha Ilmu, 2006), 111.

terhadap suatu populasi dan bukan populasi itu sendiri.[63] Selain itu terdapat dua teknik pengambilan sampel, yaitu teknik penarikan probabilita dan nonprobabilita.

Teknik penarikan probabilita yaitu suatu teknik penarikan sampel yang mendasarkan diri bahwa setiap anggota populasi memiliki kesempatan yang sama untuk dipilih sebagai sampel.[64] Dengan kesempatan yang sama ini, hasil dari suatu penelitian dapat digunakan untuk memprediksi populasi. Sementara itu, teknik penarikan sampel nonprobabilita yaitu teknik penarikan sampel yang mendasarkan pada setiap anggota populasi tidak memiliki kesempatan yang sama.[65] Dalam penelitian ini peneliti tidak dapat menentukan besarnya populasi yang akan diteliti secara pasti dikarenakan tidak terdapat data yang relevan dan juga alasan bank tidak memperbolehkan karena data nasabah juga termasuk rahasia bank. Dan peneliti mengambil sampel dalam penelitian ini adalah nasabah bank syariah dengan kisaran 30-500 sampel berdasarkan saran dari Rescoe (1975). Penelitian ini akan menggunakan teknik penarikan sampel yaitu nonprobabilita dengan metode sampling jenuh. Sampling jenuh merupakan teknik penarikan sampel jika seluruh anggota populasi dijadikan sebagai sampel, yaitu dimana terkumpul sebanyak 30 sampel yang terdiri dari pengguna internet banking pada bank syariah Mandiri (BSM Palopo), BRI Syariah dan BNI Syariah.

[63] Priyono, *Metode Penelitian Kuantitatif*, (Surabaya: Zifatama Publishing, 2016), 104.
[64] Priyono, *Metode Penelitian Kuantitatif*, (Surabaya: Zifatama Publishing, 2016), 106.
[65] Priyono, *Metode Penelitian Kuantitatif*, (Surabaya: Zifatama Publishing, 2016), 107.

E. Sumber Data

Sumber data yang digunakan dalam penelitian ini adalah berasal dari sumber data primer dan sekunder.

a. Sumber data primer

yaitu data yang hanya dapat kita peroleh dari sumber asli atau pertama[66], dalam hal ini yakni berupa angket dan google formulir yang diberikan kepada nasabah pengguna internet banking pada bank syariah Mandiri (BSM Palopo), BRI Syariah dan BNI Syariah.

b. Sumber data sekunder

yaitu data yang sudah tersedia sehingga kita tinggal mencari dan mengumpulkan.[67] Dalam hal ini diantaranya buku-buku dan jurnal terkait judul peneliti.

F. Teknik Pengumpulan Data

Survey Dengan Menggunakan Kuesioner

Kuesioner (daftar pertanyaan) Yaitu dengan cara memberikan daftar pertanyaan yang ditujukan kepada responden untuk memperoleh jawaban yang sesuai dengan penelitian.

---

[66] Jonathan Sarwono, *Metode Penelitian Kuantitatif dan Kualitatif*, (Yogyakarta: Graha Ilmu, 2006), 123.

[67] Gilang Reski Amijaya, "*Pengaruh Persepsi Teknologi Informasi, Kemudahan, Risiko, dan Fitur Layanan Terhadap Minat Ulang Nasabah Bank Dalam Menggunakan Internet Banking*", *Skripsi* (Semarang: Universitas Diponegoro, 2010), 31.

G. Taknik Analisis Data

a. Analisis kuantitatif

Penyelesaian penelitian ini menggunakan teknik analisis kuantitatif. Analisis ini dilakukan dengan cara menganalisis permasalahan yang diwujudkan dengan kuantitatif. Penyelesaikan penelitian ini dengan menggunakan teknik analisis kuantitatif karena jenis data yang digunakan adalah data kuantitatif. Adapun pengolahan data dengan analisis kuantitatif melalui beberapa tahap yaitu :

1) Uji Validitas

Uji validitas digunakan untuk menguji sejauh mana alat pengukur dapat mengungkapkan ketepatan gejala yang dapat diukur. Alat ukur yang digunakan dalam pengujian validitas adalah daftar pertanyaan yang telah diisi oleh responden dan akan diuji hasilnya guna menunjukkan valid tidaknya suatu data. Bila valid, ketetapan pengukuran data tersebut akan semakin tepat alat ukur tersebut. Kuesioner dikatakan valid apabila r hitung (*Corrected Item Total Corelation*) > r table dan kuesioner dikatakan tidak valid apabila r hitung < r table.[68] Adapun hasil dari uji validitas kuesioner peneliti yaitu sebagai berikut :

[68] Gilang Reski Amijaya, "*Pengaruh Persepsi Teknologi Informasi, Kemudahan, Risiko, dan Fitur Layanan Terhadap Minat Ulang Nasabah Bank Dalam Menggunakan Internet Banking*", *Skripsi* (Semarang: Universitas Diponegoro, 2010), 31.

Tabel 3.2

Hasil Uji Validitas

No.	Variabel	Item	R Hitung	R Tabel	Ket
1	Prinsip Kehati-hatian (X)	1	0,629	0,514	Valid
		2	0,781	0,514	Valid
		3	0,874	0,514	Valid
		4	0,766	0,514	Valid
		5	0,610	0,514	Valid
		6	0,721	0,514	Valid
		7	0,881	0,514	Valid
		8	0,764	0,514	Valid
		9	0,747	0,514	Valid
		10	0,817	0,514	Valid
2	Ancaman Situs Phising (Y)	1	0,648	0,514	Valid
		2	0,891	0,514	Valid
		3	0,726	0,514	Valid
		4	0,713	0,514	Valid
		5	0,525	0,514	Valid
		6	0,817	0,514	Valid
		7	0,786	0,514	Valid
		8	0,684	0,514	Valid
		9	0,650	0,514	Valid
		10	0,827	0,514	Valid

Sumber : Diolah menggunakan SPSS 22

2) Uji Reliabilitas

Uji reliabilitas merupakan alat untuk mengukur suatu kuesioner yang merupakan indikator dari variabel atau konstruk. Suatu kuesioner dikatakan reliable atau handal jika jawaban seseorang terhadap pertanyaan konsisten atau stabil dari waktu ke waktu. SPSS memberikan fasilitas untuk mengukur reliablitias dengan uji statistik *Cronbach Alpha (α).* Suatu variabel dikatakan reliable jika memberikan nilai α > 0,6.[69] Adapun hasil uji reabilitas kuesioner adalah sebagai berikut :

Tabel 3.3

Hasil Uji Reabilitas

No.	Variabel	Cronbach's Alpa	Ket
1	Prinsip Kehati-hatian (X)	0,776	Realibel
2	Ancaman Situs Phishing (Y)	0,772	Realibel

Sumber : Diolah menggunakan SPSS 22

H. Taknik Pengolahan Data

Teknik pengolahan menggunakan program *SPSS for Windows*. Metode analisis data yang digunakan dalam penelitian ini menggunakan uji asumsi klasik (uji normalitas, linearitas, dan heteroskedastisitas), kemudian semua data di olah dan dianalisis dengan menggunakan regresi

[69] Syofian Siregar, *"Statistik Parametrik untuk Penelitian kuantitatif"*, (Jakarta: PT Bumi Aksara, 2014), 87.

sederhana. Serta dengan uji hipotesis yang meliputi uji signifikan parameter individu (uji statistik *t*) dan uji koefisien determinasi.

a. Uji Asumsi Klasik

1) Uji Normalitas

Uji Normalitas adalah untuk melihat apakah nilai residual terdistribusi normal atau tidak. Model regresi yang baik adalah memiliki nilai residual yang terdistribusi normal. Jadi uji normalitas bukan dilakukan pada masing-masing variabel tetapi pada nilai residualnya.[70]

2) Uji Linieritas

Uji linieritas adalah analisis yang mengharuskan adanya hubungan fungsional antara X danY, pada populasi yang linear. Dalam penelitian ini perhitungan uji linieritas dengan bantuan program SPSS *for windows* dengan kriteria jika > 0,05 maka hubungan antara X dan Y dinyatakan linier. Namun jika < 0,05 maka hubungan tersebut dinyatakan tidak linier.

3) Uji Heterokedastisitas

Uji Heterokedastsitas adalah untuk melihat ada atau tidaknya korelasi yang dimana untuk melihat apakah terdapat ketidaksamaan varians dari residual satu ke pengamatan yang lain. Model regresi yang memenuhi persyaratan adalah dimana terdapat kesamaan

[70] Ansofino, dkk, *"Buku Ajar Ekonometrika"* Ed. 1 Cet. 1, (Yogyakarta: Deepublish, 2016), 94.

varians dari residual satu ke pengamatan ke pengamatan yang lain tetap atau disebut homokedastisitas.[71]

b. Analisis regresi

Analisis yang digunakan dalam penelitian ini adalah analisis regresi linear sederhana (*simple regression*). Model regresi linier sederhana adalah model probabilistik yang menyatakan hubungan linier antara dua variabel di mana salah satu variabel dianggap memengaruhi variabel lain.[72]

Secara umum persamaan regresi linear sederhana dapat dirumuskan sebagai berikut :

$$Y = a + b1X + e$$

Keterangan :

Y = Variabel terikat (Ancaman Situs *Phishing*)

X = Variabel bebas (Prinsip kehati-hatian)

a = Konstanta

b1 = Koefisien Prinsip kehati-hatian

e = error *term*

c. Uji Hipotesis

1) Uji Signifikansi Individual (Uji *t*-Statistik)

Uji *t* digunakan untuk menguji hubungan regresi secara parsial. Pengujian ini dilakukan untuk mengukur tingkat signifikan setiap variabel bebas terhadap variabel terikatnya dalam model regresi.

[71] Ansofino, dkk, *"Buku Ajar Ekonometrika"* Ed. 1 Cet. 1, (Yogyakarta: Deepublish, 2016), 94.

[72] Suyono, *"Analisis Regresi untuk Penelitian"*, (Yogyakarta: Deepublish, 2018), 5.

Pengujian ini menggunakan uji t dengan df = n-2 (30 – 2 = 28) atau df = 28 orang, dengan taraf signifikansi 5% yang artinya tingkat kesalahan suatu variabel adalah 5% atau 0,05 sedangkan tingkat keyakinannya adalah 95% atau 0,95. Maka di peroleh t_{tabel} sebesar 2,048. Jadi berdasarkan hasil yang diperoleh ditetapkanlah ketentuan:

a) Jika *T hitung <T tabel*, maka Ho diterima dan Ha ditolak, artinya tidak ada pengaruh antara variabel *independen* terhadap variabel *dependen*.

b) Jika *T hitung >T tabel*, maka Ha diterima dan Ho ditolak, artinya ada pengaruh antara variabel *independen* terhadap variabel *dependen*.

c) Apabila tingkat kesalahan suatu variabel > 5% atau 0,05 berarti variabel tersebut tidak signifikan.

d) Apabila tingkat kesalahan suatu variabel < 5% atau 0,05 berarti variabel tersebut signifikan.

2) Koefisien Determinasi R^2

Koefisien *Determinas*i adalah kemampuan model dalam menjelaskan hubungan antar variabel. Nilai koefisien determinasi adalah antara nol dan satu, semakin angka mendekati satu maka semakin baik garis regresi karena mampu menjelaskan data aktualnya, sebaliknya semakin angka mendekati nol maka kita mempunyai garis regresi

yang kurang baik. Koefisien determinasi, merupakan konsep statistik, sehingga sebuah garis regresi baik jika nilai R^2tinggi.[73]

[73] Zulfikar, "*Pengantar Pasar Modal Dengan Pendekatan Statistika"*, (Yogyakarta: Deepublish, 2016), 168.

BAB IV

HASIL DAN PEMBAHASAN

A. Sejarah Bank Syariah

Bank Syariah pada awalnya dikembangkan sebagai suatu respon dari kelompok ekonomi dan praktisi perbankan muslim yang berupaya mengakomodasi desakan dari berbagai pihak yang menginginkan agar tersedia jasa transaksi keuangan yang dilaksanakan sejalan dengan nilai moral dan prinsip-prinsip syariah Islam.[74] Perkembangan bank syariah di Sulawesi Selatan hinggal September 2019 untuk Bank Umum Syariah berjumlah 12 unit KPO/Kantor Cabang, 38 unit KCP/UPS, dan 9 unit kantor kas.[75] Kemudian untuk Unit Usaha Syariah berjumlah 9 unit KPO/Kantor Cabang, 1 unit KCP/UPS, dan 1 unit Kantor Kas.[76] Dan untuk di Kota Palopo sendiri terdapat 4 jenis bank syariah, namun peneliti hanya menggunakan 3 bank syariah saja yakni BNI Syariah Kantor cabang Mikro Palopo, Bank Syariah Mandiri, dan BRI Syariah. Di mulai dari Bank Syariah Mandiri Palopo dibuka pada Desember 2009, kemudian BNI Syariah di tahun 2010, dan setelah itu dilanjutkan dengan didirikannya BRI Syariah Palopo pada Januari 2014. Dengan masing-

[74] Agus Marimin, dkk, "Perkembangan Bank Syariah Di Indonesia", *Jurnal Ilmiah Ekonomi Islam* Vol. 1, no. 02 (2015): 75. http://www.jurnal.stie-aas.ac.id.

[75] Ernawati, "Pusat Pertumbuhan Perbankan Syariah Di Indonesia", *Jurnal Ekonomi, Manajemen, dan Akuntansi Islam* Vol. 2, no. 02 (2017): 34. http://www.researchgate.net/publication/333387762.

[76] Otoritas Jasa Keuangan, "Statistik Perbankan Syariah", Periode September 2019.

masing visi dan misi namun mempunyai tujuan yang sama yaitu mengarahkan kegiatan ekonomi ummat untuk bermuamalat secara islam.

B. Karakteristik Responden

Responden dalam penelitian ini yaitu nasabah bank syariah (BSM,BRIS,BNI Syariah) Kota Palopo baik dari kalangan mahasiswa maupun yang sudah bekerja yang menggunakan internet banking pada bank yang di maksud. Penelitian ini menggunakan 30 responden yang penulis temui pada saat penelitian dilaksanakan.

1. Karakteristik responden berdasarkan jenis kelamin

   Berikut tabel yang menggambarkan data jenis kelamin responden dari hasil kuesioner.

Tabel 4.1

Karakteristik Responden Berdasarkan Jenis Kelamin

Jenis Kelamin	Frekuensi	Persentase (%)
Laki-laki	13	43
Perempuan	17	56
Jumlah	**30**	**100**

Sumber : Data primer diolah, 2020

Berdasarkan tabel hasil menunjukkan bahwa sebesar 56% responden yang menjawab didominasi oleh jenis kelamin perempuan. Sisanya dijawab oleh responden berjenis kelamin laki-laki dengan

persentase 43%. Kondisi tersebut menandakan bahwa pengguna internet banking di bank syariah didominasi oleh perempuan.

2. Karakteristik responden berdasarkan usia

Berikut tabel yang menggambarkan data usia responden dari hasil kuesioner.

Tabel 4.2

Karakteristik Responden Berdasarkan Usia

Rentang Usia	Frekuensi	Persentase (%)
< 21 Tahun	12	40
21 – 30 Tahun	17	56
31 – 40 Tahun	1	3
41 – 50 Tahun	-	-
> 50 Tahun	-	-
Jumlah	**30**	**100**

Sumber : Data primer diolah, 2020

Berdasarkan tabel hasil menunjukkan bahwa sebesar 56% responden atau 17 orang yang menjawab didominasi oleh usia 21 – 30 tahun. Sisanya dijawab oleh responden usia <21 tahun dengan persentase 40% atau sama dengan 12 orang dan terakhir oleh usia 31 – 40 tahun dengan persentase 3% atau sama dengan 1 orang. Kondisi tersebut menandakan bahwa pengguna internet banking di bank syariah didominasi oleh usia 21 – 30 tahun.

3. Karakteristik responden berdasarkan pekerjaan

Berikut tabel yang menggambarkan data pekerjaan responden dari hasil kuesioner.

Tabel 4.3

Karakteristik Responden Berdasarkan Pekerjaan

Pekerjaan	Frekuensi	Persentase (%)
Mahasiswa	24	80
Wiraswasta	5	16
Guru	1	3
Jumlah	**30**	**100**

Sumber : Data primer diolah, 2020

Berdasarkan tabel hasil menunjukkan bahwa sebesar 80% responden atau 24 orang yang menjawab didominasi oleh mahasiswa. Sisanya dijawab oleh responden dengan profesi wiraswasta dengan persentase 16% atau sama dengan 5 orang dan terakhir oleh profesi guru dengan persentase 3% atau sama dengan 1 orang. Kondisi tersebut menandakan bahwa pengguna internet banking di bank syariah didominasi oleh mahasiswa.

4. Karakteristik responden berdasarkan jenis bank

Berikut tabel yang menggambarkan data jenis bank responden dari hasil kuesioner.

Tabel 4.4

Karakteristik Responden Berdasarkan Jenis Bank

Pekerjaan	Frekuensi	Persentase (%)
BNI Syariah	7	23
BSM	7	23
BRI Syariah	16	53
Jumlah	**30**	**100**

Sumber : Data primer diolah, 2020

Berdasarkan tabel hasil menunjukkan bahwa sebesar 53% responden atau 16 orang yang menjawab didominasi oleh BRI Syariah. Sisanya dijawab oleh responden BNI Syariah dan Bank Syariah Mandiri dengan persentase 23% atau sama dengan 7 orang. Kondisi tersebut menandakan bahwa pengguna internet banking di bank syariah didominasi oleh BRI Syariah.

C. Hasil Penelitian

1. Uji Asumsi Klasik

   a. Uji Normalitas

   Adapun hasil uji normalitas data dengan menggunakan uji *One-Sample Kolmogorov-Smirnov Test* yaitu sebagai berikut.

Tabel 4.5

Hasil Uji Normalitas Data

One-Sample Kolmogorov-Smirnov Test

		Unstandardized Residual
N		30
Normal Parameters[a,b]	Mean	.0000000
	Std. Deviation	4.91221587
Most Extreme Differences	Absolute	.114
	Positive	.085
	Negative	-.114
Test Statistic		.114
Asymp. Sig. (2-tailed)		.200[c,d]

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

d. This is a lower bound of the true significance.

Sumber : Output SPSS 22

Berdasarkan hasil uji normalitas data menggunakan metode *One-Sample Kolmogorov-Smirnov Test* didapatkan hasil nilai signifikan sebesar 0,200 dimana lebih besar (>) dari nilai signifikansi 0,05. Sehingga dapat disimpulkan bahwa uji normalitas penelitian ini terdistribusi normal.

b. Uji Linieritas

Adapun hasil uji linieritas dengan melihat *ANOVA Table* yaitu sebagai berikut.

Tabel 4.6

Hasil Uji Linieritas

ANOVA Table

			Sum of Squares	df	Mean Square	F	Sig.
Ancaman Situs Phising * Prinsip Kehati-hatian	Between Groups	(Combined)	306.583	13	23.583	3.726	.007
		Linearity	147.480	1	147.480	23.298	.000
		Deviation from Linearity	159.103	12	13.259	2.094	.084
	Within Groups		101.283	16	6.330		
	Total		407.867	29			

Sumber : Output SPSS 22

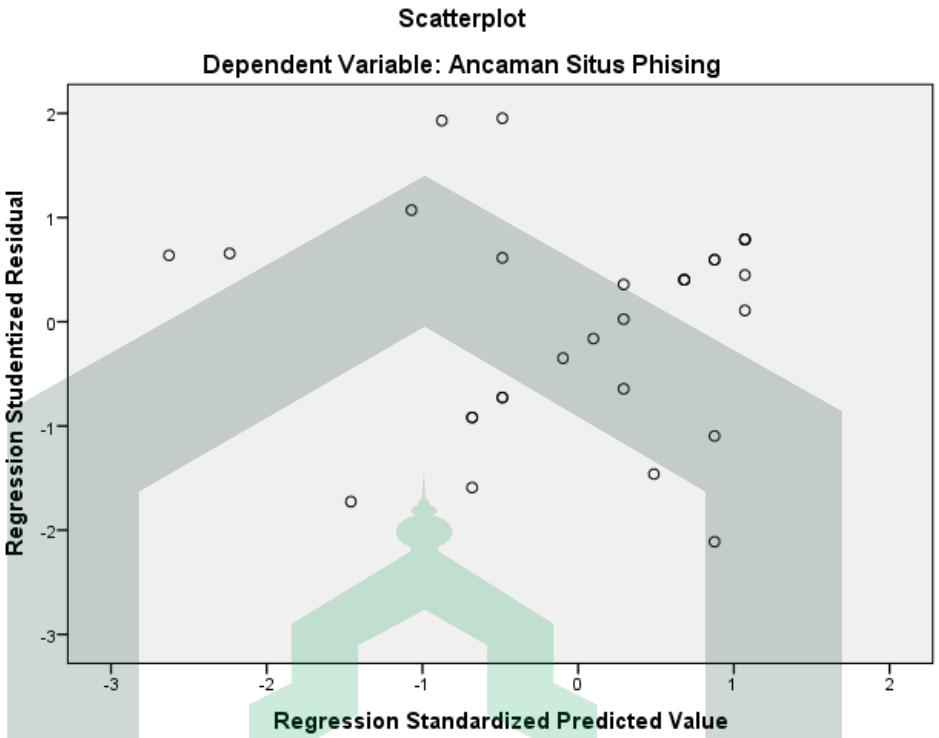
Berdasarkan Nilai siginifikansi (*Sig*) dari output diatas diperoleh nilai *Deviation from linearity Sig*. adalah 0,084 lebih besar (>) dari 0,05. Maka dapat disimpulkan bahwa hubungan antara variabel Prinsip kehati-hatian dengan variabel Ancaman Situs Phishing dinyatakan linier.

c. Uji Heteroskedastisitas

Adapun hasil uji heteroskedastisitas dengan melihat gambar *Scatterplot* yaitu sebagai berikut.

Gambar 4.1

Hasil Uji Heteroskedastisitas



Sumber : Output SPSS 22

Berdasarkan hasil *output Scatterplot* diatas menunjukkan bahwa titik-titik tersebar secara acak dan tidak membentuk pola. Dan titik penyebarannya tersebar di atas dan di bawah angka 0. Sehingga dapat disimpulkan bahwa penelitian ini tidak menunjukkan adanya gejala heteroskedastisitas.

2. Analisis Regresi

Untuk menguji apakah terdapat pengaruh variabel prinsip kehati-hatian (X) terhadap ancaman situs *phishing* (Y), maka perlu dilakukan analisis regresi sederhana yaitu sebagai berikut.

Tabel 4.7

Hasil Uji Regresi Sederhana

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	25.734	4.936		5.213	.000		
	Prinsip Kehati-hatian	.439	.110	.601	3.982	.000	1.000	1.000

a. Dependent Variable: Ancaman Situs Phising

Sumber : Output SPSS 22

Berdasarkan tabel diatas maka hasil akan dikembangkan kedalam model persamaan regresi

$$Y = a + b1X + e$$

$$Y = 25{,}734 + 0{,}439$$

Dari persamaan diatas maka dapat di interpretasikan beberapa hal yakni:

a. a = nilai konstanta : 25,734 artinya jika nilai prinsip kehati-hatian sebelum dipengaruhi oleh variabel Ancaman situs *phishing* adalah positif.
b. Koefisien B = 0,439 menunjukkan bahwasanya apabila responden positif atas variabel *reability* atau bertambah 1 maka variabel ancaman situs phising mengalami peningkatan sebesar 0,439.

3. Uji Hipotesis

a. Uji Signifikansi Individual (Uji *t*-Statistik)

Tabel 4.8

Hasil Uji *t*-Statistik

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	25.734	4.936		5.213	.000
	Prinsip Kehati-hatian	.439	.110	.601	3.982	.000

a. Dependent Variable: Ancaman Situs Phising

Sumber : Output SPSS 22

Pengujian ini menggunakan uji t dengan df = n-2 (30 – 2 = 28) atau df = 28 orang, dengan taraf signikansi 5% atau 0,05. Maka di peroleh t_{tabel} sebesar 2,048.

Berdasarkan tabel *coefficients* diatas dapat diketahui bahwa besarnya nilai *t* hitung (3,982) > nilai *t* tabel (2,048) yang berarti bahwa prinsip kehati-hatian (X) berpengaruh positif terhadap variabel ancaman situs phising (Y) dengan tingkat signifikan 0,000 < 0,05. Dengan demikian Ho ditolak dan Ha diterima, artinya variabel prinsip kehati-hatian secara parsial berpengaruh secara signifikan terhadap ancaman situs phising pada internet banking di bank syariah kota palopo.

b. Koefisien Determinasi R^2

Tabel 4.9

Hasil Uji Koefisien Determinasi

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.601[a]	.362	.339	3.050

a. Predictors: (Constant), Prinsip Kehati-hatian

b. Dependent Variable: Ancaman Situs Phising

Sumber : Output SPSS 22

Dari hasil uji koefisien determinasi (R *square*) pada tabel 4.9 tersebut jika dilihat dari *output model summary*, dapat diketahui nilai koefisien determinasi (R *square*) sebesar 0,362. Besarnya angka koefisien determinasi (R *square*) 0,362 atau sama dengan 36,2%. Angka tersebut mengandung arti prinsip kehati-hatian berpengaruh terhadap ancaman situs *phishing* sebesar 36,2%. Sedangkan sisa nya 63,8% dipengaruhi oleh variabel lain di luar model regresi ini. Besarnya pengaruh variabel lain sering disebut error (e).

D. Pembahasan

Pada penelitian ini akan dijelaskan hasil yang dimana akan menjawab rumusan masalah yang ada. Maka dari itu peneliti menggunakan data primer dengan teknik pengumpulan data dengan menyebarkan angket/kuesioner kepada responden dengan metode sampel jenuh sehingga ditemukan responden sebanyak 30 sampel. Analisis yang

peneliti gunakan dalam penelitian ini yaitu terdiri dari beberapa uji, dimulai dari Uji Asumsi klasik yang dimana terdiri dari uji normalitas, uji linieritas, dan heteroskedastisitas. Yang jabaran dari hasil uji-uji tersebut yakni pertama uji normalitas didapatkan nilai signifikan sebesar 0,200 dimana lebih besar (>) dari nilai signifikansi 0,05. Sehingga dapat disimpulkan bahwa uji normalitas penelitian ini terdistribusi normal. Kemudian yang kedua uji linieritas menunjukkan bahwa nilai *Deviation from linearity Sig*. adalah 0,084 lebih besar (>) dari 0,05. Maka dapat disimpulkan bahwa terdapat hubungan linier antara variabel Prinsip kehati-hatian dengan variabel Ancaman Situs Phising. Kemudian yang terakhir uji heteroskedastisitas dengan melihat gambar scatterplot disimpulkan bahwa penelitian ini tidak menunjukkan adanya gejala heteroskedastisitas.

Penelitian ini menggunakan analisis regresi sederhana yang kemudian dilakukan uji *t*-statistik menunjukkan hasil tabel *coefficients* diatas dapat diketahui bahwa besarnya nilai *t* hitung (3,982) > nilai *t* tabel (2,048) yang berarti bahwa prinsip kehati-hatian (X) berpengaruh positif terhadap variabel ancaman situs phising (Y) dengan tingkat signifikan 0,000 < 0,05. Dengan demikian Ho ditolak dan Ha diterima. Dari hasil tersebut diartikan bahwa prinsip kehati-hatian merupakan salah satu variabel yang berpengaruh terhadap ancaman situs phishing. Semakin tinggi nilai prinsip kehati-hatian maka semakin kuat pengaruhnya dari ancaman situs phishing.

Penelitian ini relevan dengan penelitian yang dilakukan oleh Yulia Naili Rahmah (2018) yaitu Pengaruh Penggunaan *Internet Banking* dan Perlindungan Nasabah Pengguna Fasilitas *Internet Banking* Terhadap *Cybercrime* Di Daerah Istimewa Yogyakarta (DIY), dengan hasil penelitian yaitu perhitungan secara parsial pengaruh *Client Charter* terhadap *Cybercrime* diperoleh nilai koefisien regeresi sebesar -0,591.[77] Pada taraf signifikansi 5%, dapat diketahui *t* hitung sebesar -2,341 dengan nilai signifikansi sebesar 0,022, karena koefisien regresi mempunyai nilai negatif dan nilai signifikansi (p) < 0,05 maka hipotesis "Terdapat pengaruh Client Charter terhadap Cyber Crime di Daerah Istimewa Yogyakarta" diterima.[78]

[77] Yulia Naili Rahma, "*Pengaruh Penggunaan Internet Banking dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cybercrime Di Daerah Istimewa Yogyakarta(DIY)", Skripsi* (Universitas Negeri Yogyakarta Juni 2018): 86.

[78] Yulia Naili Rahma, "*Pengaruh Penggunaan Internet Banking dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cybercrime Di Daerah Istimewa Yogyakarta(DIY)", Skripsi* (Universitas Negeri Yogyakarta Juni 2018): 87.

BAB V

KESIMPULAN

A. Kesimpulan

Berdasarkan pembahasan hasil penelitian dan uji statistik, maka dapat ditarik kesimpulan yaitu variabel prinsip kehati-hatian (X) berpengaruh positif terhadap variabel ancaman situs *phishing* (Y) dengan tingkat signifikan 0,000 < 0,05 serta nilai koefisien determinasi (R *square*) sebesar 0,362 atau sama dengan 36,2%. Angka tersebut mengandung arti prinsip kehati-hatian berpengaruh terhadap ancaman situs *phishing* sebesar 36,2% dan hasil uji *t*-statistik yaitu nilai *t* hitung (3,982) > nilai *t* tabel (2,048) sehingga dapat diartikan Ho ditolak dan Ha diterima.

B. Saran

1. Bagi Praktis

Bagi Bank Syariah terkhusus Kota Palopo diharuskan memberikan dan mempertahankan keamanan dalam pelayanan pada internet banking agar terhindarkan dari risiko kejahatan *cybercrime*, dan bagi nasabah itu sendiri agar mengetahui dan memahami bahaya-bahaya dari kejahatan internet yang bisa saja terjadi jika nasabah lalai dalam menggunakan produk internet banking.

2. Bagi Akademik

Untuk penelitian selanjutnya, penelitian ini dapat dilakukan penambahan variabel selain yang dibahas pada peneltian ini agar dapat memberikan pengetahuan tertentu mengenai kejahatan-kejahatan di dunia internet banking. Penelitian ini dapat dijadikan bahan referensi bagi pihak kampus sebagai bahan acuan penelitian yang akan datang selain jurnal dan buku yang sudah ada.

DAFTAR PUSTAKA

Aboobucker, Ilmudeen, and Yukun Bao. "What Obstruct Costomer Acceptance of Internet Banking? Security and Privacy, Risk, Trust and Website Usability and The Role of Moderators." *Journal of High Technology Management Research* xxx (xxxx) (2018): 2. https://www.researchgate.net/publication/324777661_What_obstruct_customer_acceptance_of_internet_banking_Security_and_privacy_risk_trust_and_website_usability_and_the_role_of_moderators.

Abubakar, Lastuti, and Tri Handayani. "Telaah Yuridis Terhadap Implementasi Prinsip Kehati-Hatian Bank Dalam Aktivitas Perbankan Indonesia." *De Lega Lata* Vol. 2 no. (2017): 69. https://doi.org/https://doi.org/10.31219/osf.io/acxqu.

Amijaya, Gilang Reski. "Pengaruh Persepsi Teknologi Informasi, Kemudahan, Risiko, Dan Fitur Layanan Terhadap Minat Ulang Nasabah Bank Dalam Menggunakan Internet Banking." Universitas Diponegoro, 2010.

Ansofino, and Dkk. *Buku Ajar Ekonometrika*. Ed. 1, Cet. Yogyakarta: Deepublish, 2016.

Arifin, H. Djohar. "Pengaruh Internet Banking Terhadap Tingkat Kepercayaan Nasabah Pada Bank Bri Syariah Kcp Arjawinangun." *Al-Amwal* Vol 8, No. (2016): 533. https://syekhnurjati.ac.id/jurnal/index.php/amwal/article/view/1610.

Astuti, Rahma Yudi. "Penerapan Prinsip Kehati-Hatian Dalam Penyaluran Pembiayaan Dan Kredit Pada Lembaga Keuangan Mikro (Studi Multi Situs Pada BMT Hasanah Mlarak Dan BRI Unit Mlarak, Ponorogo)." *Al Tijarah* Vol. 2 no. (2016): 31. http://ejournal.unida.gontor.ac.id/index.php/altijarah/article/download.

Chandra, Cherry Agustine, and I Gede Suwetja. "Teks Peran BI Terhadap Transfer Dana Melalui Sistem Kliring Nasional PT. Bank Sulutgo." *Jurnal Ipteks Akuntansi Bagi Masyarakat* Vol 2, No. (2018): 643–44. https://media.neliti.com/media/publications/294269-ipteks-peran-bi-terhadap-transfer-dana-m-e08358af.

Dariyani, Ririn Irma. "Implementasi Strategic Corporate Social Responsibility Dalam Perspektif Shari'ah Enterprise Theory." *Dinamika Global: Rebranding Keunggulan Kompetitif Berbasis Kearifan Lokal* ISBN 978-6 (2016): 846. http://jurnal.unej.ac.id/index.php/prosiding/article/download.

Departemen Pendidikan Nasional. *Kamus Besar Bahasa Indonesia*. Ed. 3. Balai Pustaka, 2005.

Djanggih, Hardianto, and Nurul Qamar. "Penerapan Teori-Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (Cybercrime)." *Pandecta* Vol 13 No. (2018): 20. https://doi.org/http://dx.doi.org/10.15294/pandecta.v13i1.14020.

DZ, Abdul Salam. "Inklusi Keuangan Perbankan Syariah Berbasis Digital-Banking: Optimalisasi Dan Tantangan." *Al-Amwal* Vol. 10, N (2018): 64–65. http://syekhnurjati.ac.id/jurnal/index.php/amwal/article/view/2813.

Ernawati. "Pusat Pertumbuhan Perbankan Syariah Di Indonesia." *Rnal Ekonomi, Manajemen, Dan Akuntansi Islam* Vol. 2, no (2017): 34. http://www.researchgate.net/publication/333387762.

Fadzlurrahman, Etty Mulyati, Helza Nova Lita. "J-HES Penerapan Prinsip Kehati-Hatian Terhadap Kepatuhan Syariah Oleh Penyelenggara Teknologi Finansial." *Jurnal Hukum Ekonomi Syariah (J-HES)* Vol 4, no. 02 (November 29, 2020): 180–97. https://jurnal.unismuh.ac.id/index.php/jhes/article/view/4213.

Gan, Gerald Goh Guan. "Phishing: A Growing Challenge for Internet Banking Providers in Malaysia." *Communications of the IBIMA* Vol. 5 (2008): 140. http://ibimapublishing.com/articles/CIBIMA/2008/252213/252213.

Ginanjar, Aseh, Nur Widiyasono, and Gunawan Rohmat. "Analisis Serangan Web Phising Pada Layanan E-Commerce Dengan Metode Network Forensic Process." *JUTEI* Vo. 2, No. (2018): 147. https://jutei.ukdw.ac.id/index.php/jurnal/article/view/111.

Hakimi, Rifqy. "Studi Isu Keamanan Jaringan Pada Facebook." *Jurnal Pustakawan Indonesia* Vol. 11, n (2012): 8. https://journal.ipb.ac.id/index.php/jpi/article/view/11421.

Jansen, Jurjen, and Rutger Leukfeldt. "Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization." *International Journal of Cyber Criminology* Vol. 10, n (2016): 80. http://www.cybercrimejournal.com/Jansen&Leukfeldtvol10issue1IJCC2016.

Kementrian Agama Republik Indonesia. *Al-Qur'an Dan Terjemahnya*. Bandung: Fokus Media, 2010.

Koskoas, Ioannis V. "E-Banking Security: A Communication Perspective." *Risk Management* Vol. 13, N (2011): 83. https://www.researchgate.net/publication/261945762_Ebanking_security_A_communication_perspective.

———. "Trust and Risk Communication in Setting Internet Banking Security Goals." *Risk Management* Vol. 10, N (2008): 59–60. https://www.researchgate.net/publication/32042765_Trust_and_Risk_Communication_in_Setting_Internet_Banking_Security_Goals.

Kusnanto, Yudhi. "Analisis Kerentanan Dan Kehandalan Layanan Jaringan Cloud Berbasis Platform Eucalyptus." *Jurnal Sistem Informasi (JSI)* Vol. 8, no (2016): 46. http://ejournal.unsri.ac.id/index.php/jsi/index.

Marimin, Agus, Abdul Haris Romdhoni, and Tira Nur Fitria. "Perkembangan Bank Syariah Di Indonesia." *Jurnal Ilmiah Ekonomi Islam* Vol. 1, no (2015): 75. http://www.jurnal.stie-aas.ac.id.

Mehendele, Deepashree K., Reshma S. Masurekar, Neeta Takawale, and Shibani Kulkarni. "Review of Phishing Attacks and Anti Phishing Tools." *International Journal Of Innovative Research In Computer And Communication Engineering (IJRCCE)* Vol. 5, no (2017): 15132. http://www.ijircce.com/upload/2017/september/49_Final_Paper _16.

Murfi, Rosmida, and Teguh Suripto. "Analisa Minat Mahasiswa Terhadap

Penggunaan Layanan Internet Banking Bank BNI Syariah." *Jurnal Ekonomi Syariah Indonesia* Vol. X, No (2020): 58. https://ejournal.almaata.ac.id/index.php/JESI/article/view/1349/1337.

Otoritas Jasa Keuangan. "Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum," 20–23, 2016.

———. "Statistik Perbankan Syariah," n.d.

Permana, Angga Aditya, and Desi Nurnaningsih. "Application of Cryptography With Data Encryption Standard (DES) Algorithm in Picture." *JIKA (Jurnal Informatika)* Vol 4, No. (2020): 83. http://jurnal.umt.ac.id/index.php/jika/article/view/2640/1762.

Priyono. *Metode Penelitian Kuantitatif*. Surabaya: Zifatama Publishing, 2016.

Purwaningrum, Fajar Adhi, Agus Purwanto, and Eko Agus Darmadi. "Optimalisasi Jaringan Menggunakan Firewall." *Jurnal IKRA - ITH Informatika* Vol 2, No. (2018): 19. https://journals.upi-yai.ac.id/index.php/ikraith-informatika/article/download/251/144.

Purwiantono, Febry Eka. "Model Klasifikasi Untuk Deteksi Situs Phising Di Indonesia." Institut Teknologi Sepuluh November, 2017.

Rachmawati, Dian. "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber." *Jurnal SAINTIKOM* Vol. 13, n (2014): 211. https://prpm.trigunadharma.ac.id/public/fileJurnal/hpG3Jurnal Dian Rahmawaty2014.

Radiansyah, Ikhsan, Candiwan, and Yudi Priyadi. "Analyze Phising Threats in Online Banking Service," 2016.

Rahma, Yulia Naili. "Pengaruh Penggunaan Internet Banking Dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cybercrime Di Daerah Istimewa Yogyakarta(DIY)." Universitas Negeri Yogyakarta, 2018.

Reddy, E. Konda, Dr. Rajaman, and Dr. V. Vijaya Saradhi. "Detecting Of E-Banking Phishing Websites." *International Journal of Modern Engineering Research (IJMER)* Vol. 2, No (2012): 46. http://www.ijmer.com/papers/vol2_issue1/I021046054.pdf.

Republika.co.id. "Rekening Pelaku Phising Nasabah Mandiri Bengkulu Dibekukan." Accessed January 21, 2020. https://republika.co.id/berita/nsuvn6257/rekening-pelaku-emphisingem-nasabah-mandiri-bengkulu-dibekukan.

Rosmalinda. "Prinsip Kehati-Hatian Dalam Perspektif Pencegahan Pembiayaan Mudharabah Bermasalah Di BPRS Bumi Rinjani Malang." UIN Sunan Kalijaga, 2011. http://digilib.uin.suka.ac.id/7017/&ved=2ahUKEwiuluDNgt3oA.

Rozali, Asep. "Prinsip Mengenal Nasabah (Know Your Costumer Principle) Dalam Praktik Perbankan." *Jurnal Wawasan Hukum* Vol. 24, N (2011): 304. http://ejournal.sthb.ac.id/index.php/jwy/article/download/18.

Sarwono, Jonathan. *Metode Penelitian Kuantitatif Dan Kualitatif*. Yogyakarta: Graha, 2006.

Siregar, Syofian. *Statistik Parametrik Untuk Penelitian Kuantitatif*. Jakarta: PT

Bumi Aksara, 2014.

Stephan, Walter G, Oscar Ybarra, and Kimberly Rios Morrison. "Intergroup Threat Theory." Wikipedia, 2009. https://en.wikipedia.org/wiki/Integrated_threat_theory.

Suganya, V. "A Review on Phishing Attacks and Various Anti Phishing Techniques." *International Journal of Computer Applications* Vol. 139, (2016): 23. https://www.ijcaonline.org/archives/volume139/number1/24454-2016909084.

Sugiyono. *Metode Penelitian Bisnis (Pendekatan Kuantitatif, Kualitatif, Dan R&D)*. Bandung: CV Alfabeta, 2013.

Suyono. *Analisis Regresi Untuk Penelitian*. Yogyakarta: Deepublish, 2018.

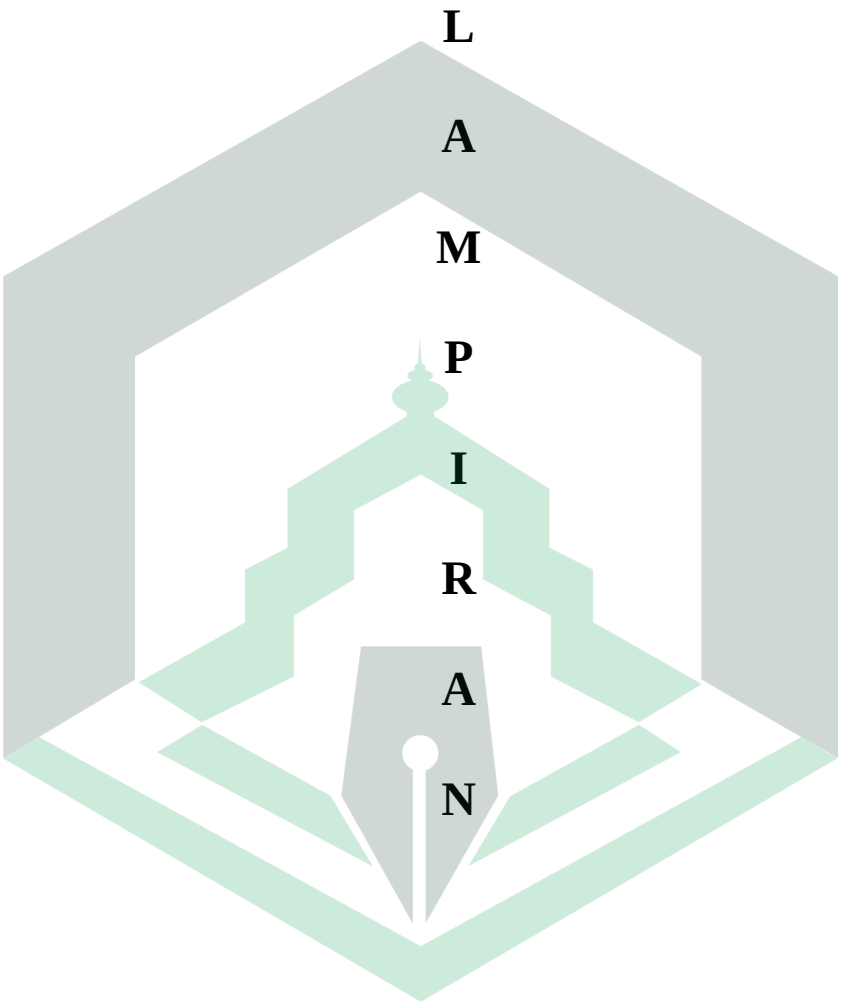
Syed, Alhussan O. Al, and Anwar L. Bilgrami. "E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities." *International Journal of Emerging Technology and Advanced Engineering* Vol 7, no. (2017): 114. http://www.cybercrimejournal.com/Jansen&Leukfeldtvol10issue1IJCC2016.

Vyctoria. *Bongkar Rahasia E-Banking Security Dengan Teknik Hacking Dan Carding*. Ed. 1. Yogyakarta: Andi Offset, 2013.

Widyarini, Lydia Arie. "Analisis Niat Perilaku Menggunakan Internet Banking Di Kalangan Pengguna Internet Di Surabaya." *Jurnal Widya Manajemen & Akuntansi* Vol 5, No. (2005): 109–10. http://journal.wima.ac.id/index.php/JWMA/article/view/1177.

Yusmad, Muammar Arafat. *Aspek Hukum Perbankan Syariah Dari Teori Ke Praktik*. Ed. 1 Cet. Yogyakarta: Deepublish, 2017.

Zulfikar. *Pengantar Pasar Modal Dengan Pendekatan Statistika*. Yogyakarta: Deepublish, 2016.


L
A
M
P
I
R
A
N

IAIN PALOPO

KUESIONER PENELITIAN

INSTITUT AGAMA ISLAM NEGERI PALOPO
FAKULTAS EKONOMI DAN BISNIS ISLAM
PROGRAM STUDI PERBANKAN SYARIAH

Assalamu'Alaikum Warahmatullahi Wabarakatuh

Nama : Andi Siti Nurbaya Sari

NIM : 16 0402 0013

Program Studi : Perbankan Syariah

Fakultas : Ekonomi dan Bisnis Islam

Perguruan Tinggi : Institut Agama Islam Negeri Palopo

Saat ini saya sedang melakukan penelitian untuk skripsi saya mengenai **"Pengaruh Prinsip Kehati-hatian Terhadap Ancaman Situs Phishing Pada Nasabah Pengguna Internet Banking"**. Situs Phisihing itu sendiri merupakan aktivitas membujuk atau memancing nasabah melalui via email, telepon maupun chat untuk mengunjungi dan mengakses sebuah situs atau link yang dimana link tersebut merupakan situs web palsu yang dapat meretas informasi pribadi nasabah bank. Saya selaku peneliti meminta kesediaan Bapak/Ibu/Saudara/i untuk membantu penelitian ini dengan mengisi kuesioner. Berikut kuesioner yang saya ajukan, mohon kepada Bapak/Ibu/Saudara/i untuk memberikan jawaban yang sejujur-jujurnya dan sesuai dengan keadaan yang sebenarnya. Informasi atau data yang diperoleh bersifat rahasia dan hanya akan dipergunakan untuk penelitian ini. Atas kesediannya saya ucapkan terima kasih.

Wasalamu'Alaikum Warahmatullahi Wabarakatuh

Penulis,

Andi Siti Nurbaya Sari
NIM. 16.0402.0013

PROFIL RESPONDEN

Isi dan berikan tanda silang (X) pada kotak yang tersedia dibawah ini.

1. Nama :
2. Jenis Kelamin : □ Laki-Laki □ Prempuan
3. Usia : □ < 21 Tahun

IAIN PALOPO

KUESIONER PENELITIAN

INSTITUT AGAMA ISLAM NEGERI PALOPO
FAKULTAS EKONOMI DAN BISNIS ISLAM
PROGRAM STUDI PERBANKAN SYARIAH

		□ 21 – 30 Tahun	□ 41 – 50 Tahun
		□ 31 – 40 Tahun	□ > 50 Tahun
4.	Nasabah dari bank	: □ BRI Syariah	□ BNI Syariah
		□ BSM	□ ……

A. Petunjuk Pengisian

1. Sebelum mengisi kuesioner ini, mohon Bapak/Ibu membaca setiap butir pernyataan dengan cermat.
2. Silahkan beri tanda *check list* (✓) pada kolom yang sesuai dengan pilihan.
3. Untuk setiap butir pernyataan hanya diperbolehkan memilih satu alternative jawaban.
4. Jika ada kesalahan dalam memilih alternative jawaban, beri tanda (X) pada kolom yang salah kemudian beri tanda *check list* (✓) pada kolom yang sesuai.
5. Semua pernyataan yang ada, mohon dijawab tanpa ada satupun yang lewat.

B. Keterangan Jawaban

Untuk menjawab pertanyaan berikut, silahkan disesuaikan dengan skala penilaian berikut.

SINGKATAN	KETERANGAN	NILAI
SS	Sangat Setuju	5
S	Setuju	4
RR	Ragu-ragu	3
TS	Tidak Setuju	2
STS	Sangat Tidak Setuju	1

IAIN PALOPO

KUESIONER PENELITIAN

INSTITUT AGAMA ISLAM NEGERI PALOPO
FAKULTAS EKONOMI DAN BISNIS ISLAM
PROGRAM STUDI PERBANKAN SYARIAH

PERTANYAAN PENELITIAN

1. Apakah anda pernah/sedang menggunakan Internet Banking ?
   - □ Ya
   - □ Tidak
2. Apakah anda sudah paham tentang Situs Phishing ?
   - □ Ya
   - □ Tidak

I. PRINSIP KEHATI-HATIAN

NO	PERNYATAAN	JAWABAN				
		SS	S	RR	TS	STS
		5	4	3	2	1
TRANSPARANSI						
1	Saya dengan mudah untuk mengakses aplikasi/web dan mendapatkan informasi terkait pembaharuan aplikasi					
2	Penggunaan website resmi perbankan sebagai sarana publikasi informasi terbaru bank ke publik					
3	Pengumuman atau informasi rekening dapat diakses setiap waktu					
4	Bank menyampaikan informasi produk dan jasa, menerapkan pengelolaan pengaduan nasabah dengan efektif serta memelihara data dan informasi pribadi nasabah secara memadai					
RESPONSIBILITY						
1	Jasa yang ada pada layanan online banking pada bank syariah sesuai dengan yang saya butuhkan					
2	Saya percaya layanan online banking bank syariah memiliki sistem keamanan yang baik					
3	Saya percaya informasi dan masukan yang diberikan oleh bank					
4	Saya percaya rekening dan data saya aman di bank					

IAIN PALOPO

KUESIONER PENELITIAN
INSTITUT AGAMA ISLAM NEGERI PALOPO
FAKULTAS EKONOMI DAN BISNIS ISLAM
PROGRAM STUDI PERBANKAN SYARIAH

KEWAJARAN						
1	Bank memberikan kesempatan kepada seluruh nasabah untuk memberikan masukan saran pada kotak dialog yang tersedia pada fitur online banking serta mempunyai akses terhadap informasi sesuai prinsip keterbukaan					
2	Bank senantiasa memperhatikan kepentingan seluruh nasabah berdasarkan asas kewajaran					

II. ANCAMAN SITUS PHISHING

NO	PERNYATAAN	JAWABAN				
		SS	S	RR	TS	STS
		5	4	3	2	1
PENGETAHUAN						
1	Ancaman situs phishing dapat disebabkan oleh pelaku cyber yang mengirimkan alamat web palsu kedalam e-mail/pesan chat dengan menggunakan identitas bank					
2	Bahaya dari ancaman situs phishing dapat terbongkarnya informasi pribadi nasabah serta data sensitif seperti username dan password					
3	Motivasi terjadinya ancaman phishing karena banyaknya penyalahgunaan teknologi					
4	Cara terhindar dari ancaman phishing yaitu dengan memperhatikan sumber dari pengirim e-mail/pesan, dan melihat perbedaan website asli dengan tiruan					
5	Apabila menerima pesan yang mencurigakan dan meminta untuk melakukan verifikasi registrasi password atau aktivasi data, akan sangat berguna jika kita menghubungi pihak customer service bank secara langsung					
PSIKOLOGI						
1	Saya merasa takut dengan adanya ancaman situs phishing pada online banking					
2	Situs phishing membuat saya ragu untuk menggunakan fasilitas online banking					

IAIN PALOPO

KUESIONER PENELITIAN

INSTITUT AGAMA ISLAM NEGERI PALOPO
FAKULTAS EKONOMI DAN BISNIS ISLAM
PROGRAM STUDI PERBANKAN SYARIAH

3	Saya mencari tahu tentang bahaya ancaman situs phishing pada media sosial maupun berita					
4	Saya mulai belajar membedakan alamat web resmi perbankan dengan yang tiruan untuk menghindari terjadinya ancaman situs phishing					
5	Maraknya kasus phishing yang terjadi karena kecanggihan dan praktisnya teknologi sehingga banyak oknum yang menyalahgunakan kemudahan tersebut untuk kepentingan pribadi					

~ TERIMA KASIH ATAS PARTISIPASINYA ~

HASIL KUESIONER PENELITIAN
Pengaruh Prinsip Kehati-Hatian terhadap Ancaman Situs Phishing pada Nasabah Pengguna Internet Banking

Responden	Data Responden																					
	Prinsip kehati-hatian											Ancaman Situs Phishing										
	1	2	3	4	5	6	7	8	9	10	X	1	2	3	4	5	6	7	8	9	10	Y
1	2	1	2	4	4	4	2	4	4	4	31	4	3	3	5	4	4	4	4	5	5	41
2	5	3	3	3	4	3	3	3	3	3	33	5	4	3	5	3	5	4	3	5	5	42
3	5	5	4	5	5	5	5	5	5	5	49	5	4	3	5	4	5	4	5	4	5	44
4	5	4	4	3	3	4	4	3	5	4	39	4	5	4	5	5	5	4	5	4	5	46
5	5	5	5	5	5	5	5	5	5	5	50	5	5	4	5	5	4	5	5	5	5	48
6	5	5	5	5	4	5	5	5	5	5	49	4	5	3	4	5	4	5	4	5	5	44
7	5	4	4	5	5	5	4	5	5	5	47	2	4	4	3	5	4	4	5	4	4	39
8	5	3	5	5	4	5	4	5	5	5	46	3	3	4	3	4	4	5	4	4	4	38
9	5	5	4	4	4	4	4	4	4	4	42	2	1	2	4	4	4	2	4	4	4	31
10	5	4	5	5	5	5	4	5	5	5	48	5	3	3	3	4	3	3	3	3	3	33
11	5	5	5	5	5	5	5	5	5	5	50	5	5	4	5	5	5	5	5	5	5	49
12	4	4	3	3	4	4	4	5	5	5	41	5	4	4	3	3	4	4	3	5	4	39
13	5	3	4	3	5	5	3	4	5	5	42	5	5	5	5	5	5	5	5	5	5	50
14	5	5	5	5	5	4	5	5	5	5	49	5	5	5	5	4	5	5	5	5	5	49
15	5	4	5	5	5	4	4	4	5	5	46	5	4	4	5	5	5	4	5	5	5	47
16	5	4	5	5	5	5	4	5	5	5	48	5	4	5	5	5	5	4	5	5	5	48
17	5	5	5	5	5	5	5	5	5	5	50	5	5	5	5	5	5	5	5	5	5	50
18	4	4	3	3	4	4	4	5	5	5	41	4	4	3	3	4	4	4	5	5	5	41
19	5	3	4	3	5	5	3	4	5	5	42	5	3	4	3	5	5	3	4	5	5	42
20	5	4	4	4	4	3	4	4	4	4	40	5	5	5	5	5	4	5	5	5	5	49
21	5	2	4	5	5	3	3	4	5	5	41	5	2	4	5	5	3	3	4	5	5	41
22	5	5	5	5	5	5	5	5	5	5	50	5	5	5	5	5	5	5	5	5	5	50
23	5	5	4	5	5	4	1	5	5	5	44	5	5	4	5	5	4	1	5	5	5	44
24	5	5	5	5	5	5	5	5	5	5	50	5	5	5	5	5	5	5	5	5	5	50
25	5	4	5	4	4	5	4	5	5	5	46	5	4	5	4	4	5	4	5	5	5	46
26	4	4	3	3	4	3	4	4	4	4	37	4	4	3	3	4	3	4	4	4	4	37
27	5	5	5	5	5	4	5	5	5	5	49	5	5	5	5	5	4	5	5	5	5	49
28	5	5	4	4	5	5	5	5	5	5	48	5	5	4	4	5	5	5	5	5	5	48
29	5	4	3	5	4	4	4	4	4	5	42	5	4	3	5	4	4	4	4	4	5	42
30	5	5	4	4	5	4	4	5	4	5	45	5	5	4	4	5	4	4	5	4	5	45

Titik Persentase Distribusi t (df = 1 – 40)

Pr	0.25	0.10	0.05	0.025	0.01	0.005	0.001
df	0.50	0.20	0.10	0.050	0.02	0.010	0.002
1	1.00000	3.07768	6.31375	12.70620	31.82052	63.65674	318.30884
2	0.81650	1.88562	2.91999	4.30265	6.96456	9.92484	22.32712
3	0.76489	1.63774	2.35336	3.18245	4.54070	5.84091	10.21453
4	0.74070	1.53321	2.13185	2.77645	3.74695	4.60409	7.17318
5	0.72669	1.47588	2.01505	2.57058	3.36493	4.03214	5.89343
6	0.71756	1.43976	1.94318	2.44691	3.14267	3.70743	5.20763
7	0.71114	1.41492	1.89458	2.36462	2.99795	3.49948	4.78529
8	0.70639	1.39682	1.85955	2.30600	2.89646	3.35539	4.50079
9	0.70272	1.38303	1.83311	2.26216	2.82144	3.24984	4.29681
10	0.69981	1.37218	1.81246	2.22814	2.76377	3.16927	4.14370
11	0.69745	1.36343	1.79588	2.20099	2.71808	3.10581	4.02470
12	0.69548	1.35622	1.78229	2.17881	2.68100	3.05454	3.92963
13	0.69383	1.35017	1.77093	2.16037	2.65031	3.01228	3.85198
14	0.69242	1.34503	1.76131	2.14479	2.62449	2.97684	3.78739
15	0.69120	1.34061	1.75305	2.13145	2.60248	2.94671	3.73283
16	0.69013	1.33676	1.74588	2.11991	2.58349	2.92078	3.68615
17	0.68920	1.33338	1.73961	2.10982	2.56693	2.89823	3.64577
18	0.68836	1.33039	1.73406	2.10092	2.55238	2.87844	3.61048
19	0.68762	1.32773	1.72913	2.09302	2.53948	2.86093	3.57940
20	0.68695	1.32534	1.72472	2.08596	2.52798	2.84534	3.55181
21	0.68635	1.32319	1.72074	2.07961	2.51765	2.83136	3.52715
22	0.68581	1.32124	1.71714	2.07387	2.50832	2.81876	3.50499
23	0.68531	1.31946	1.71387	2.06866	2.49987	2.80734	3.48496
24	0.68485	1.31784	1.71088	2.06390	2.49216	2.79694	3.46678
25	0.68443	1.31635	1.70814	2.05954	2.48511	2.78744	3.45019
26	0.68404	1.31497	1.70562	2.05553	2.47863	2.77871	3.43500
27	0.68368	1.31370	1.70329	2.05183	2.47266	2.77068	3.42103
28	0.68335	1.31253	1.70113	2.04841	2.46714	2.76326	3.40816
29	0.68304	1.31143	1.69913	2.04523	2.46202	2.75639	3.39624
30	0.68276	1.31042	1.69726	2.04227	2.45726	2.75000	3.38518
31	0.68249	1.30946	1.69552	2.03951	2.45282	2.74404	3.37490
32	0.68223	1.30857	1.69389	2.03693	2.44868	2.73848	3.36531
33	0.68200	1.30774	1.69236	2.03452	2.44479	2.73328	3.35634
34	0.68177	1.30695	1.69092	2.03224	2.44115	2.72839	3.34793
35	0.68156	1.30621	1.68957	2.03011	2.43772	2.72381	3.34005
36	0.68137	1.30551	1.68830	2.02809	2.43449	2.71948	3.33262
37	0.68118	1.30485	1.68709	2.02619	2.43145	2.71541	3.32563
38	0.68100	1.30423	1.68595	2.02439	2.42857	2.71156	3.31903
39	0.68083	1.30364	1.68488	2.02269	2.42584	2.70791	3.31279
40	0.68067	1.30308	1.68385	2.02108	2.42326	2.70446	3.30688