Contents list available at: https://ejournal.iainpalopo.ac.id/index/
Journal of Institution and Sharia Finance
Journal homepage: https://ejournal.iainpalopo.ac.id/index.php/sharia_finance

Analysis Prudential Principles About The Treath of Phishing Sites For Internet Banking Customers

Andi Siti Nurbaya Sari

Institusi Agama Islam Negeri Palopo, Palopo, Indonesia

Article Info

Keywords:
Phisisng Sites, Precautionary Principles, Internet

Paper type:
Research Paper

Corresponding author:
sari@gmail.com

Abstract

This thesis is motivated by the existence of an internet site that refers to the act of luring internet banking users to visit fake websites designed by cyber-cybers that resemble the official website in such a way as to trick victims through fake emails (or instant messages) and then secretly take the victim's personal information. . Seeing this requires the precautionary principle regulated by banks to find out customer identities, monitor customer transaction activities including reporting suspicious transactions. The type of research used is the Quantitative Method with 30 samples using a nonprobability sampling technique, namely saturated samples. The instrument used is a questionnaire (questionnaire). Data were processed and analyzed using simple linear regression using SPSS 22 for windows. The results showed that the precautionary principle had a positive effect on the threat of phishing sites by 36.2% with t count (3.982) t table (2.048) with a significant level of 0.000 <0.05. This means that the precautionary principle variable partially has a significant effect on the threat of phishing sites on internet banking at Islamic banks in Palopo city. So it can be concluded that with the precautionary principle of the bank and for customers it can reduce the risk of phishing site threats and more guaranteed security of customer data on internet banking at Islamic banks in Palopo city.

Cite this document:
Sari, A. S. N. (2021). Analysis Prudential Principles About The Treath of Phishing Sites For Internet Banking Customers. *Journal of Institution and Sharia Finance, 4* (1). 26-38. https://doi.org/10.24256/joins.v4i1.3378

Analisis Prinsip Kehati-Hatian Terhadap Ancaman Situs Phishing pada Nasabah Pengguna Internet Banking

Abstrak

Riset ini dilatarbelakangi dengan 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 dengan 30 sampel 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.

Keywords: *Situs Phisisng, Prinsip Kehati-Hatian, Internet.*

PENDAHULUAN

Perbankan didunia saat ini elah memakai teknologi Mutahir, dimana bisa diakses lewat jejaring social manapun. Melihat hal tersebut bank pemerintah serta bank swasta mengambil kesempatan dengan memandang persaingan kedepanny, (Amijaya, 2010). 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, sebagaimana yang telah dikemukakan oleh World Economic Forum (2015). Dalam hal 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 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. Selain itu saat ini telah diciptakan *fintech* lending untuk perbankan dalam mempraktikkan *Digital Branch* yang full digital di kantor cabang bank secara umum. Dengan demikian, menurut Koskosas (2011) 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. 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.

Aboobucker (2018) mengatakan pentingnya meningkatkan keamanan dalam sistem informasi karena sistem ini menjadi sensitif terhadap lingkungan dan dapat membuat organisasi sangat rentan terhadap serangan system. Walaupun kemampuan manfaat yang ditawarkan *internet banking* kepada nasabah penerimaan layanannya sudah terbatas serta dalam banyak permasalahan kandas penuhi harapan. Berdasarkan hal tersebut dapat diperediksikan mengakibatkan adanya 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 pada aksi menyerang yang menarik pengguna untuk mendatangi website palsu dengan mengirimi mereka email palsu (ataupun pesan praktis) serta secara diam-diam untuk 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* kamu serta kata sandi lewat hyperlink yang disediakan dalam email (Reddy, 2012). 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 menerapka prinsip syariah secara tidak langsung telah melaksanakan bagian dari prinsip kehati-hatian. Kehati-hatian sendiri berguna untuk menanggulangi risiko yang mungkin akan terjadi dalam lembaga keuangan syariah. Menurut Rosali (2011) prinsip yang dianut bank adalah mengidentifikasi nasabah dan memantau aktivitas transaksi nasabah, termasuk melaporkan transaksi yang mencurigakan.

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. Selain itu prinsip kehati-hatian bagi bank berguna untuk melindungi data nasabah serta terhindar dari praktik-praktik penipuan 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".

Ikhsan Radiansyah, Candiwan, dan Yudi Priyadi (2016) dalam penelitiannya yang berjudul analisis ancaman *Phising* dalam layanan *online banking* menjelaskan bahwa pengetahuan pengguna yang minim dan psikologi pengguna serta privasi social networking service pengguna merupakan faktor penyebab adanya *Phising*. Selain itu menurut Penelitian oleh Fadzlurrahman, Etty Mulyati, Helza Nova Lita (2020) dalam penelitiannya 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. Berdasarkan penelitian terdahulu tersebut dalam penelitian ini membahas leih lanjut penyebab Phishing terhadap layanan internet banking dengan memperhitungkan pengaruh prinsip kehati-hatian terhadap ancaman situs Phishing pada nasabah pengguna internet banking.

LITERATUR REVIEW

Self Service Technology (Teknologi Berbasis Layanan Mandiri)

Yang et al, (2011) 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.

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) yang dikutip dalam jurnal Dariyani dalam judul *Implementasi Strategic Corporate Social Responsibility Dalam Perspektif Shari'ah* 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).

Teori Anomi

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. 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 (Dianggi 2018). 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)

Prinsip kehati-hatian ialah sebuah asas yang mengungkapkan bahwasanya dalam menjalankan kegiatan usaha serta fungsinya, bank wajib bersikap hati-hati guna melindungi dana masyarakat yang diamanahkan padanya. Menurut Rosmalinda (2011) prinsip kehati-hatian bank juga merupakan prinsip yang dalam mengoperasikan usahanya agar dalam kondisi kinerja yang baik dan memenuhi kriteria bank yang sehat. 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 (Rozali, 2011). Selain itu prinsip kehati-hatian bagi bank berguna untuk melindungi data nasabah serta terhindar dari praktik-praktik penipuan.

Ancaman

Sebuah teori menurut Stephan dan Renfro (2009) 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 dirasakan mencakup semua ancaman yang diyakini anggota kelompok mereka alami, terlepas dari apakah ancaman itu benar-benar ada. 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.

Situs Phising

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. 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 (Reddy, 2011). Kemudian menurut Leukfeldt (2015) dalam 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. Phishing adalah sebuah aktifitas kriminal dalam mencuri informasi pribadi yang sifatnya sensitif seperti username dan password melalui penyamaran sebagai entitas yang terpercaya dan membuat korbantidak sadar telah memberikan informasi sensitif ke scammer (Radiansyah, 2016). Ada beberapa hal yang perlu dicermati agar terhindar dari serangan phising:

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.

Internet Banking

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. Menurut Widyarini (2005) 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.

METODE PENELITIAN

Penelitian ini menggunakan penelitian kuantitatif dengan tenik pengambilan sampel secara random dengan kisaran 30-500 dimana populasi yang digunakan peneliti yaitu nasabah bank Syariah dengan Teknik penarikan sampel menggunakan *nonprobability* dengan metode sampel 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. Adapun sumber data yang digunakan yaitu berasal dari data primer dan sekunder. Teknik pengumpulan data peneliti dengan cara penyebaran kuesioner yang ditujukan kepada responden untuk memperoleh jawaban yang sesuai dengan penelitian. Selain itu analisis data yang digunakan menggunakan bantuan SPSS Windows sebagai alat untuk menguji validitas, reliabilitas serta digunakan dalam teknik pengelolahan data yaitu uji asumsi klasik yang terdiri dari uji normalitas, linearitas, dan heteroskedastisitas Serta uji hipotesis dengan analisis regresi sederhana untuk memperoleh hasil penelitian dan menarik kesimpulan penelitian peneliti.

HASIL DAN PEMBAHASAN

Uji Normalitas

Tabel 1. 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.

Uji lineritas

Tabel 2. Hasil Uji Linieritas

ANOVA Table

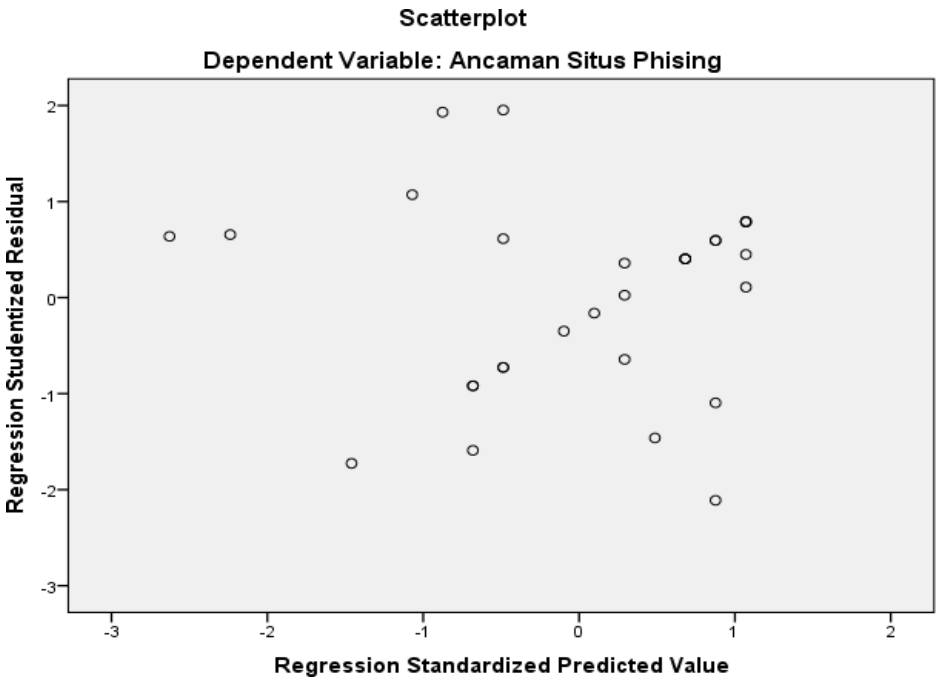
			Sum of Squares	df	Mean Square	F	Sig.
Ancaman Situs Phising * Prinsip Kehati-hatian	Between Groups	(Combined)	306.583	13	23.583	3.726	.007
		Linearity	147.480	1	147.480	23.298	.000
		Deviation from Linearity	159.103	12	13.259	2.094	.084
	Within Groups		101.283	16	6.330		
	Total		407.867	29			

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.

Uji Heteroskedastisitas



Gambar 1. Hasil Uji Heteroskedastisitas

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.

Analisis Regresi

Tabel 3. 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.

Hipotesis
Uji Signifikansi Individual (Uji t-Statistik)

Tabel 4. 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.

Koefisien Determinasi R^2

Tabel 5. 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).

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 (Rahma, 2018).

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.

Berdasarkan pada penelitan tersebut Adapun saran pada penelitian ini perbankan 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.

DAFTAR PUSTAKA

Aboobucker, Ilmudeen., 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*. 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_moderat ors.

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

Dariyani, Ririn Irma. 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.

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.

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.

Jansen, Jurjen 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.

Koskosas, Ioannis V. 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_pers pective.

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

Radiansyah, Ikhsan dkk, Analyze Phising Threats in Online Banking Service‖, Paper (Universitas Telkom, 2016): 1

Rahma, Yulia Naili. 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

Reddy, E.konda 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.

Rozali, Asep. 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.

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

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

Widyarini Lydia Arie, 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.