



**PERLINDUNGAN HUKUM BAGI KORBAN TINDAK PIDANA  
*CYBER CRIME PHISHING***

SKRIPSI



Oleh:  
**Khanifah Jannatul Diniyah**  
**21801021087**

**UNIVERSITAS ISLAM MALANG  
FAKULTAS HUKUM  
MALANG  
2022**

### ABSTRACT

*This research is motivated by the rise of cases of phishing circulating in the community. cases Phishing circulating in the community are very detrimental, both material and moral losses. The legal issue raised in this research is how to regulate cyber crime phishing in Indonesia and a form of legal protection for its victims. This research is a normative juridical law research through a statutory approach, a conceptual approach and a case approach. The collection of legal materials is done through the literature study method. Sources of legal materials consist of primary, secondary and tertiary legal materials. The legal material obtained is then analyzed and processed to be compiled systematically. The results of the study indicate that the regulation of cyber crime phishing is regulated in the Criminal Code and the ITE Law, and legal protection can be obtained from Article 378 of the Criminal Code, Article 28 paragraph (1) and Article 35 of the ITE Law and Article 40 of Law Number 36 of 1999 concerning Telecommunications.*

**Keywords:** *Legal Protection, Crime, Cyber crime, Phishing*

### ABSTRAK

Penelitian ini dilatarbelakangi oleh maraknya kasus-kasus *phishing* yang beredar di masyarakat. Kasus-kasus *phishing* yang beredar di masyarakat sangat merugikan, baik itu kerugian secara materil maupun moril. Isu hukum yang diangkat dalam penelitian ini adalah bagaimana bentuk pengaturan tindak pidana *cyber crime phishing* di Indonesia dan bentuk perlindungan hukum bagi korbannya. Penelitian ini merupakan penelitian hukum yuridis normatif melalui pendekatan perundang-undangan, pendekatan konseptual dan pendekatan kasus. Pengumpulan bahan hukum dilakukan melalui metode studi literatur. Sumber bahan hukum terdiri dari bahan hukum primer, sekunder dan tersier. Bahan hukum yang diperoleh kemudian dianalisis dan diolah untuk disusun secara sistematis. Hasil penelitian menunjukkan bahwa pengaturan tindak pidana *cyber crime phishing* diatur dalam KUHP dan UU ITE, serta perlindungan hukum dapat diperoleh dari pasal 378 KUHP, Pasal 28 ayat (1) serta pasal 35 UU ITE dan pasal 40 UU Nomor 36 Tahun 1999 tentang Telekomunikasi.

**Kata Kunci:** *Perlindungan Hukum, Tindak Pidana, Cyber crime, Phishing*

## BAB I PENDAHULUAN

### A. Latar Belakang Masalah

Dalam era modern seperti sekarang ini, internet merupakan suatu hal yang tidak dapat dipisahkan dalam kehidupan sehari-hari di masyarakat. Keberadaan internet tentu saja semakin memudahkan kehidupan. Banyak hal yang dapat dilakukan dengan internet. Misalnya sebagai sarana komunikasi, *e-money*, internet banking, dan masih banyak lagi. Internet sudah menjadi kebutuhan hidup di hampir sebagian besar masyarakat. Terutama dalam keadaan pandemi yang melanda dunia seperti sekarang ini. Internet telah menghadirkan realitas kehidupan baru kepada manusia. Internet telah mengubah jarak dan waktu menjadi tidak terbatas. Dengan internet, manusia dapat melakukan berbagai aktivitas yang dalam dunia nyata sulit dilakukan.

Seiring dengan semakin populernya internet, masyarakat penggunanya seakan-akan mendapati suatu dunia baru yang dinamakan *cyber space*. Alam baru yang terbentuk oleh media internet ini pada perkembangannya menciptakan masyarakat baru yang sering disebut sebagai *netizen*.<sup>1</sup> Disamping banyaknya manfaat serta kemudahan yang didapatkan dari penggunaan internet, tak jarang pula terdapat hal negatif yang ditimbulkan dari penggunaan internet ini sendiri. Untuk melindungi dan menghormati hak-hak masyarakat dibidang kebebasan serta memberikan keadilan yang merata bagi seluruh masyarakat dengan pertimbangan keamanan dan ketertiban umum, kemudian dibentuklah Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang

---

<sup>1</sup> Ki Jagad Tomara (2013), Skripsi Fakultas Hukum Universitas Brawijaya, Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet dan Pemilik Domain Situs *Phishing*, hlm 3

Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik agar terwujud keadilan, ketertiban umum, dan kepastian hukum.

UU ITE bermaksud untuk melindungi hak dan kewajiban bagi para pengguna internet. Karena kejahatan tidak hanya ada pada dunia nyata tetapi juga di dunia maya. Kejahatan yang dilakukan dengan media internet ini dikenal pula dengan istilah *cyber crime*. *Cyber crime* sendiri adalah suatu bentuk kejahatan yang dilakukan menggunakan jaringan komputer sebagai unsur utamanya. Hingga hari ini kasus kejahatan di dunia maya (*cyber crime*) semakin bertambah, modusnya pun makin beragam, serta makin bervariasi karakteristik pelaku kejahatannya, dan makin serius akibatnya.<sup>2</sup> Bentuk kejahatan di dunia maya atau *cyber crime* bermacam-macam, berikut uraiannya.

1. Pertama: mengandung kekerasan (*cyber crime with violence*), diantaranya adalah:
  - a. *Cyber terrorism, Assault by Threat* (serangan terorisme dunia maya),
  - b. *Cyber stalking* (penguntitan dunia maya),
  - c. *Child Pornography* (pornografi pada anak).
2. Kedua: tanpa kekerasan (*cyber without violence*), diantaranya adalah:
  - a. *Cyber trespass* (memasuki jaringan secara ilegal),
  - b. *Cyber thief* (pencurian dunia maya),
  - c. *Cyber fraud* (penipuan dunia maya),
  - d. *Destructive Cyber crimes* (perusakan jaringan),
  - e. *Cyber Prostitute Ads* (iklan prostitusi *online*),
  - f. *Cyber gambling* (perjudian *online*),

---

<sup>2</sup> Widodo (2013), *Memerangi Cybercrime Karakteristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi*, Asswaja Pressindo, Yogyakarta, hlm, 1.

- g. *Cyber Drugs Sales* (penjualan obat & narkoba di internet),
- h. *Cyber Laundering* (pencucian uang),
- i. *Cyber Phishing* (pencurian data pribadi antara lain berawal dari penipuan berupa link/situs *web site*).<sup>3</sup>

*Phishing* merupakan salah satu kejahatan maya paling populer. Melansir artikel bebas *Phishing.org* dalam salah satu esainya yang berjudul *What is Phishing?*, *Phishing* didefinisikan sebagai kejahatan dunia maya di mana seseorang yang menyamar sebagai institusi resmi pemerintah mendekati korban/target melalui email, telepon, atau pesan teks, meminta data sensitif seperti informasi identitas pribadi, informasi perbankan dan kartu kredit, serta kata sandi. Informasi tersebut kemudian digunakan untuk mendapatkan akses ke akun sensitif seperti bank, data pribadi, yang berpotensi mengakibatkan pencurian identitas dan kerugian finansial.<sup>4</sup>

*Phishing*, atau pencurian data elektronik, adalah perolehan informasi pribadi yang tidak sah seperti ID pengguna, PIN, nomor rekening bank, atau nomor kartu kredit. Penipu kemudian akan menggunakan informasi ini untuk mendapatkan akses ke akun, melakukan penipuan kartu kredit, atau mengarahkan klien untuk melakukan transfer ke akun tertentu dengan imbalan hadiah. Berikut ini diambil dari Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik:

- Pasal 32 ayat (2)

---

<sup>3</sup> Hilman Mursidi (2019), Skripsi Fakultas Hukum Universitas Sriwijaya, Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana *Cyber Crime Phishing* (Studi Kasus Putusan Pengadilan Negeri Medan Nomor : 3006/Pid.Sus/2017/PN.Mdn ), hlm 5

<sup>4</sup> Jerat Hukum Pelaku *Phishing* dan Modusnya, diakses pada Rabu 26 Mei 2021 dari: <https://www.hukumonline.com/klinik/detail/ulasan/cl5050/jerat-hukum-pelaku-iphishing-i-dan-modusnya/>



Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

- Pasal 35

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.

- Pasal 48 ayat (2)

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp. 3.000.000.000,00 (tiga miliar rupiah).

- Pasal 51 ayat (1)

Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp. 12.000.000.000,00 (dua belas miliar rupiah).

Adapun beberapa pasal yang berpotensi menjerat pelaku, antara lain:<sup>5</sup>

- Penipuan

Penipuan diatur dalam Pasal 378 KUHP, dengan bunyi sebagai berikut:

Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang

---

<sup>5</sup> *Ibid*

maupun menghapuskan piutang, diancam karena penipuan, dengan pidana penjara paling lama 4 tahun.

- Manipulasi

Pelaku yang melakukan *phishing* dengan cara mengirimkan surat elektronik (*e-mail*) yang seolah-olah asli dapat dijerat Pasal 35 jo. Pasal 51 UU ITE, sebagai berikut:

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik dipidana penjara paling lama 12 tahun dan/atau denda paling banyak Rp. 12 miliar.

- Penerobosan

Jika pelaku menerobos atau menjebol suatu sistem elektronik tertentu, menggunakan identitas dan password korban dengan tanpa hak, ia dapat dijerat Pasal 30 ayat (3) jo. Pasal 46 ayat (3) UU ITE, sebagai berikut:

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan dipidana penjara paling lama 8 tahun dan/atau denda paling banyak Rp. 800 juta.

- Memindahkan atau Mentransfer

Atas perbuatan memindahkan atau mentransfer informasi dan/atau dokumen elektronik milik korban, misalnya isi rekening, pelaku dapat dijerat Pasal 32 ayat (2) jo. Pasal 48 ayat (2) UU ITE yang berbunyi:

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak dipidana penjara paling lama 9 tahun dan/atau denda paling banyak Rp. 3 miliar.

Pengaruh kemajuan dari penjelasan diatas, Teknologi Internet mampu mengubah berbagai pola-pola yang sudah mapan dalam suatu tindak pidana dengan kata lain modus operandi yang umumnya dilakukan dalam kejahatan konvensional melalui teknologi internet telah diubah menjadi modus operandi yang sifatnya baru, sehingga hal ini mengakibatkan perlunya ditemukan upaya-upaya penanganan yang baru pula.<sup>6</sup>

Dengan semakin majunya peradaban manusia, sebagai implikasi dari perkembangan ilmu pengetahuan dan teknologi, muncul berbagai kejahatan berdimensi baru yang termasuk didalamnya adalah *phishing*. Sejalan dengan itu diperlukan upaya penanggulangan untuk menjamin ketertiban dalam masyarakat. Dalam perspektif hukum upaya ini dilakukan dengan hukum pidana yang kemudian memunculkan istilah *cyber law* untuk pengaturan tindak pidana yang melibatkan internet sebagai medianya.

Perkembangan teknologi serta perkembangan masyarakat telah membawa perubahan pada pola hidup masyarakat, sehingga hukum perlu untuk mengikutinya. Oleh karena itu diatur pula mengenai hukum pidana khususnya mengenai tindak pidana yang kemudian disertai dengan ancaman sanksi pidananya. Pemberian sanksi dilakukan sesuai dengan ketentuan pidana yang berlaku menurut undang-undang yang bersangkutan.

Pidana selain dimaksudkan untuk memberikan penderitaan kepada pelaku tindak pidana serta memberikan efek jera kepada pelakunya, juga dapat digunakan sebagai peringatan kepada masyarakat agar tidak melakukan kejahatan yang serupa serta senantiasa waspada dan berhati-hati dalam bertingkah laku.

---

<sup>6</sup> Hilman Mursidi, *op cit*



Di Indonesia sendiri kejahatan di dunia maya sudah diatur dalam suatu undang-undang khusus, yaitu Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Didalam undang-undang ini telah diatur berbagai hal yang berkaitan dengan suatu informasi elektronik beserta kriteria-kriterianya.

Namun seiring berjalannya waktu jumlah kejahatannya bukan semakin berkurang namun makin bertambah dan berkembang. Modusnya pun beragam, serta kejahatannya mulai merambah ke berbagai bidang, sehingga korban kejahatannya pun meningkat. Hal inilah yang kemudian menarik minat penulis untuk melakukan penelitian mengenai “PERLINDUNGAN HUKUM BAGI KORBAN TINDAK PIDANA *CYBER CRIME PHISHING*”.

#### **B. Rumusan Masalah**

Rumusan masalah yang diangkat dalam penelitian ini diantaranya sebagai berikut:

1. Bagaimana pengaturan tindak pidana *Cyber Crime Phishing* di Indonesia?
2. Bagaimana perlindungan hukum bagi korban tindak pidana *Cyber Crime Phishing*?

#### **C. Tujuan Penelitian**

Dalam setiap kegiatan penelitian tentu ada suatu tujuan yang dimaksudkan.

Adapun tujuan dari penulisan penelitian ini adalah:

1. Untuk mengetahui bagaimana bentuk pengaturan tindak pidana *cyber crime phishing* di Indonesia.
2. Untuk mengetahui bagaimana bentuk perlindungan hukum bagi korban tindak pidana *cyber crime phishing*.

#### D. Manfaat Penelitian

Dalam suatu penulisan tentunya diharapkan adanya manfaat yang dapat diperoleh baik itu bagi penulis sendiri maupun bagi masyarakat yang membacanya. Oleh karena itu penulis mengharapkan tulisan ini membawa manfaat yaitu:

##### 1. Manfaat Teoritis

Penulis berharap agar penelitian ini dapat bermanfaat untuk menambah serta memperluas wawasan di bidang hukum pidana mengenai perlindungan hukum bagi korban tindak pidana *Cyber Crime Phishing*. Penelitian ini dapat menjadi bahan kajian dalam melakukan penelitian tentang isu hukum yang relevan. Penulis berharap tulisan ini dapat diterima di kalangan akademis khususnya di bidang ilmu hukum pidana dalam menerapkan ilmu pengetahuan dan tambahan literatur dalam hukum pidana khususnya mengenai tindak pidana *Cyber Crime Phishing*.

##### 2. Manfaat Praktis

Hasil penelitian ini diharapkan dapat menambah sumbangan ilmu pengetahuan dan literatur dalam melakukan penyelidikan dan penyidikan mengenai tindak pidana *Cyber Crime Phishing* serta dapat menjadi pertimbangan bagi peristiwa-peristiwa baru yang berkaitan untuk mewujudkan kepastian hukum di Indonesia. Selain itu diharapkan dapat membantu masyarakat yang mengalami peristiwa serupa dengan penelitian ini.

#### E. Orisinalitas Penelitian

1	NAMA PENULIS	JUDUL KARYA ILMIAH	JENIS KARYA ILMIAH	TAHUN	INSTANSI
---	--------------	--------------------	--------------------	-------	----------

KI JAGAD TOMARA	KAJIAN YURIDIS PERTANGGUNGJAW ABAN PIDANA PENYEDIA JASA INTERNET DAN PEMILIK DOMAIN SITUS <i>PHISHING</i>	SKRIP SI	2011	UNIVERSIT AS BRAWIJAY A
<b>ISU HUKUM</b>				
<ol style="list-style-type: none"> <li>1. Peraturan hukum apa saja dalam sistem hukum pidana di Indonesia yang dapat digunakan untuk menjerat pelaku <i>phishing</i>?</li> <li>2. Bagaimana pertanggungjawaban pelaku sebagai pemilik website (domain) dalam hukum pidana?</li> <li>3. Bagaimana bentuk pertanggungjawaban ISP sebagai penyedia jasa internet sekaligus sebagai penyedia halaman web (<i>web hosting</i>) yang memuat konten <i>phishing</i> dalam hukum pidana?</li> </ol>				
<b>HASIL PENELITIAN</b>				
<ol style="list-style-type: none"> <li>1. Ketentuan perundangan yang dapat digunakan untuk menjerat pelaku <i>phishing</i> menurut KUHP yaitu ketentuan pasal 378 bagi perbuatan penipuan; ketentuan pasal 263 ayat (1) bagi perbuatan pemalsuan surat; ketentuan pasal 362 bagi perbuatan pencurian. Sedangkan ketentuan perundangan yang dapat digunakan untuk menjerat pelaku <i>phishing</i> menurut UU ITE yaitu ketentuan pasal 28 ayat (1), dengan ancaman sanksi pidana sesuai pada ketentuan pasal 45 ayat (2) bagi perbuatan penipuan; ketentuan pasal 35, dengan ancaman sanksi pidana sesuai pada ketentuan pasal 51 ayat (1) bagi perbuatan pemalsuan surat; ketentuan pasal 30 ayat (3), dengan ancaman sanksi pidana sesuai pada ketentuan pasal 46 ayat (3) bagi perbuatan penerobosan; ketentuan pasal 32 ayat (2), dengan ancaman sanksi pidana sesuai pada ketentuan pasal 48 ayat (2) bagi perbuatan pencurian. Pada UU ITE dikenal adanya pemberatan hukuman terutama yang berkaitan dengan sistem pembebanan pertanggungjawaban pada korporasi, terutama pada ketentuan pasal 52 ayat (4), dimana hal ini tidak diatur dalam KUHP.</li> </ol>				

	<p>2. Pelaku sebagai pemilik domain mutlak dapat dipertanggungjawabkan dalam tindak pidana <i>phishing</i>, mengingat isi dan materi dalam website menjadi tanggungjawab sepenuhnya oleh pemilik website itu sendiri. Bentuk pertanggungjawabannya sesuai dengan ketentuan yang terdapat dalam KUHP maupun UU ITE.</p> <p>3. Penyedia jasa internet sebagai penyedia jasa tidak dapat turut dipersalahkan apabila pengguna jasanya terbukti melakukan tindak pidana. Apabila terbukti turut berpartisipasi dalam perbuatan pidana tersebut, maka penyedia jasa internet dapat dikenai pertanggung jawaban pidana. Karena penyedia jasa internet merupakan sebuah korporasi, maka pembebanan pertanggung jawabannya menggunakan sistem pertanggung jawaban korporasi.</p>
<b>PERSAMAAN</b>	: Mengkaji tindak pidana <i>Cyber Crime Phishing</i>
<b>PERBEDAAN</b>	: Objek kajiannya tentang kajian yuridis pertanggungjawaban pidana penyedia jasa internet dan pemilik domain situs <i>phishing</i>
<b>KONTRIBUSI</b>	: Memberikan kontribusi bagi perkembangan ilmu hukum pidana, khususnya berkaitan dengan masalah pertanggungjawaban pidana bagi pemilik website (domain) yang berisi konten <i>phishing</i>

2	<b>NAMA PENULIS</b>	<b>JUDUL KARYA ILMIAH</b>	<b>JENIS KARYA ILMIAH</b>	<b>TAHUN</b>	<b>INSTANSI</b>
	HILMAN MURSIDI	PERTANGGUNGJAWABAN PIDANA TERHADAP PELAKU TINDAK PIDANA <i>CYBER CRIME</i>	SKRIPSI	2019	UNIVERSITAS SRIWIJAYA

	<p><i>PHISHING</i> (STUDI KASUS PUTUSAN PENGADILAN NEGERI MEDAN NOMOR : 3006/Pid.Sus/2017/PN.Mdn)</p>			
<b>ISU HUKUM</b>				
<ol style="list-style-type: none"> <li>1. Bagaimana pengaturan tindak pidana <i>Cyber Crime Phishing</i> ditinjau dalam hukum positif Indonesia?</li> <li>2. Bagaimana pertanggungjawaban pidana terhadap pelaku tindak pidana <i>Cyber Crime Phishing</i>?</li> </ol>				
<b>HASIL PENELITIAN</b>				
<p>Dengan Putusan No: 3006/Pid.Sus/2017/PN.Mdn, Majelis Hakim Pengadilan Negeri Medan memutuskan untuk menjatuhkan hukuman kepada pelaku kejahatan siber, yang diawali dengan <i>phishing</i> dengan tujuan menyebarkan ujaran kebencian dan menyebarkan berita bohong atau <i>hoax</i>. Dalam Pasal 45 ayat (3) Undang-Undang Nomor 19 Tahun 2016 Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Hakim Pengadilan Negeri Medan menjatuhkan pidana penjara 1 (satu) tahun dikurangi dengan selama terdakwa dalam tahanan sementara dengan perintah untuk tetap ditahan.</p>				
<p><b>PERSAMAAN</b> : Mengkaji tindak pidana <i>Cyber Crime Phishing</i></p>				
<p><b>PERBEDAAN</b> : Objek kajian berupa studi kasus putusan Pengadilan Negeri Medan Nomor: 3006/Pid.Sus/2017/PN.Mdn</p>				
<p><b>KONTRIBUSI</b> : Untuk dapat mencegah dan mengatasi kasus-kasus kejahatan internet yang semakin marak di masyarakat dan bermanfaat sebagai bahan evaluasi bagi penegak hukum dalam memberantas kejahatan, serta menyadarkan masyarakat akan partisipasinya untuk lebih peka terhadap kasus-kasus yang terjadi di masyarakat saat ini, dan untuk mengetahui</p>				



	peraturan perundang-undangan yang menjadi batasan dalam penggunaan internet untuk dipatuhi dan diperhatikan,
--	--

Sedangkan penelitian ini adalah

<b>1</b>	<b>NAMA PENULIS</b>	<b>JUDUL KARYA ILMIAH</b>	<b>JENIS KARYA ILMIAH</b>	<b>TAHUN</b>	<b>INSTANSI</b>
	KHANIFAH JANNATUL DINYAH	PERLINDUNGAN HUKUM BAGI KORBAN TINDAK PIDANA <i>CYBER CRIME PHISHING</i>	SKRIPSI	2021	UNIVERSITAS ISLAM MALANG
<b>ISU HUKUM</b>					
<ol style="list-style-type: none"> <li>1. Bagaimana pengaturan tindak pidana <i>Cyber Crime Phishing</i> di Indonesia?</li> <li>2. Bagaimana perlindungan hukum bagi korban tindak pidana <i>Cyber Crime Phishing</i>?</li> </ol>					
<b>NILAI KEBARUAN</b>					
<p>Penelitian ini berbeda dengan kedua penelitian yang telah dijelaskan di atas. Penelitian pertama berfokus pada studi hukum pertanggungjawaban pidana pemilik domain situs <i>phishing</i> dan penyedia jasa internet, sedangkan penelitian kedua berfokus pada studi kasus Putusan Pengadilan Negeri Medan Nomor: 3006/Pid.Sus/2017/PN.Mdn, sedangkan penelitian ini hanya membahas kejahatan siber dalam bentuk <i>phishing</i> sesuai dengan Undang-Undang Nomor 11 Tahun 2008 dan lebih mendetail tentang perlindungan hukum bagi korbannya.</p>					

#### F. Metode Penelitian

Menurut Soerjono Soekanto penelitian hukum merupakan kegiatan ilmiah yang didasarkan pada metode, sistematika dan pemikiran tertentu, yang bertujuan

untuk mempelajari satu atau beberapa gejala umum hukum tertentu dengan jalan menganalisisnya. Di samping itu juga diadakan pemeriksaan mendalam terhadap fakta hukum tersebut kemudian mengusahakan suatu pemecahan atas permasalahan-permasalahan.<sup>7</sup>

Pengertian sederhana dari metode penelitian adalah tata cara bagaimana melakukan penelitian. Metode penelitian membicarakan mengenai tata cara pelaksanaan penelitian.<sup>8</sup> Untuk menyelesaikan penelitian ini metode penelitian yang digunakan penulis yaitu:

#### 1) Jenis Penelitian

Penulis dalam menyelesaikan penelitian ini menggunakan jenis penelitian yuridis normatif. Penelitian hukum normatif diartikan sebagai penelitian atas aturan-aturan perundangan, baik ditinjau dari sudut hierarki perundang-undangan (vertikal) maupun hubungan harmoni perundang-undangan (horizontal).<sup>9</sup>

Pengertian lain dari penelitian yuridis normatif atau penelitian hukum normatif adalah penelitian yang berfokus pada norma-norma hukum yang berlaku dan pengkajian norma-norma hukum tersebut dilakukan dengan cara meneliti data sekunder sebagai data utama, sedangkan data primer sebagai penunjang. Adapun jenis pendekatannya sebagai berikut:

#### 2) Jenis Pendekatan

Penelitian ini menggunakan 3 macam pendekatan, yakni pendekatan perundang-undangan (*statute approach*), pendekatan konseptual (*conseptual*

<sup>7</sup> Zaenudin Ali, 2010, Metode Penelitian Hukum, Sinar Grafika, Jakarta, hlm 18.

<sup>8</sup> Jonaedi Efendi, Johnny Ibrahim, 2018, Metode Penelitian Hukum Normatif dan Empiris, Prenada Media, Jakarta, hlm 2

<sup>9</sup> Elisabeth Nurhaini Butarbutar, 2018, Metode Penelitian Hukum, Refika Aditama, Bandung, hlm 83

*approach*), dan pendekatan kasus (*case approach*). Penelitian hukum normatif disebut juga penelitian kepustakaan atau studi dokumen, karena penelitian ini dilakukan atau ditujukan hanya pada peraturan-peraturan tertulis atau bahan-bahan hukum yang lain.<sup>10</sup>

### 3) Sumber Bahan Hukum

Terdapat tiga macam sumber bahan hukum yang digunakan oleh penulis untuk menyelesaikan penelitian ini. Sumber bahan hukum tersebut yaitu:

#### a. Bahan Hukum Primer

Bahan hukum primer merupakan bahan hukum yang bersifat autoratif, artinya, mempunyai otoritas. Bahan hukum terdiri dari perundang-undangan, catatan-catatan resmi.<sup>11</sup> Adapun undang-undang yang penulis gunakan sebagai acuan penelitian ini adalah:

1. Kitab Undang-Undang Hukum Pidana (KUHP)
2. Kitab Undang-Undang Hukum Acara Pidana
3. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
4. Undang-Undang Nomor 31 Tahun 2014 tentang Perubahan Atas Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban
5. Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

#### b. Bahan Hukum Sekunder

---

<sup>10</sup> *Ibid*, hlm 84

<sup>11</sup> Suratman dan Phillips Dilla, 2015, *Metode Penelitian Hukum*, Alfabeta Bandung, Bandung hlm 65

Bahan hukum sekunder adalah dokumen atau bahan hukum yang memberikan penjelasan terhadap bahan hukum primer seperti buku-buku, artikel, jurnal, hasil penelitian, makalah dan lain sebagainya yang relevan dengan permasalahan yang akan dibahas.<sup>12</sup>

Bahan hukum yang penulis gunakan dalam penelitian ini berasal dari jurnal hukum dan sumber dari internet yang dapat dipertanggungjawabkan tulisannya.

c. Bahan Hukum Tersier

Bahan hukum tersier sebagai bahan hukum yang memberikan petunjuk dan penjelasan terhadap bahan hukum primer dan sekunder, seperti kamus, maupun ensiklopedi.<sup>13</sup>

4) Teknik Pengumpulan Bahan Hukum

Bahan hukum dikumpulkan melalui prosedur inventarisasi dan identifikasi peraturan perundang-undangan, serta klasifikasi dan sistematisasi bahan hukum sesuai permasalahan penelitian. Oleh karena itu, teknik pengumpulan bahan hukum yang digunakan dalam penelitian ini adalah dengan studi kepustakaan.<sup>14</sup>

Studi kepustakaan merupakan suatu metode penelitian yang menggunakan dokumen sebagai sumber datanya. Adapun sumber informasinya dapat berupa jurnal hukum, hasil dari penelitian hukum, laporan, dan berbagai literatur yang relevansi dari beberapa buku yang berkaitan dengan rumusan masalah penelitian

---

<sup>12</sup>Pengenalan Bahan Hukum, diakses pada Kamis 27 Mei 2021 dari [https://simdos.unud.ac.id/uploads/file\\_penelitian\\_1\\_dir/7847bff4505f0416fe0c446c60f7e8ac.pdf](https://simdos.unud.ac.id/uploads/file_penelitian_1_dir/7847bff4505f0416fe0c446c60f7e8ac.pdf)

<sup>13</sup> *Ibid*

<sup>14</sup>Metode Penulisan, diakses pada Kamis 27 Mei 2021 dari: <http://repository.umy.ac.id/bitstream/handle/123456789/23062/BAB%20III.pdf?sequence=4&isAllowed=y>

ini. Bahan hukum yang diperoleh kemudian dikumpulkan dengan menggunakan studi dokumentasi.

#### 5) Teknik Analisis Bahan Hukum

Analisis bahan hukum merupakan langkah-langkah yang berkaitan dengan pengolahan bahan-bahan yang diperoleh, baik itu studi kepustakaan maupun studi lapangan untuk mencari jawaban atas isu hukum yang dipermasalahkan dalam penelitian. Data yang diperoleh dalam penelitian ini dianalisis secara deskriptif kualitatif.

Deskriptif maksudnya pengambilan data yang diperoleh dari hasil penelitian bahan hukum diolah dan disusun secara sistematis dan diuraikan, sehingga diperoleh gambaran yang jelas dan lengkap tentang obyek penelitian. Sedangkan kualitatif maksudnya data yang diperoleh dipisah-pisahkan, diambil yang memiliki relevansi dengan permasalahan untuk kemudian dikaji lebih lanjut dan disusun secara sistematis sehingga diperoleh kesimpulan.<sup>15</sup>

#### G. Sistematika Penulisan

Untuk memberikan kemudahan bagi pembaca untuk memahami isi penelitian ini, penulis akan menjabarkan sistematika penulisan penelitian ini sebagai berikut:

#### BAB I: PENDAHULUAN

Dalam bab pendahuluan ini penulis uraikan tentang latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, orisinalitas penelitian, metode penelitian, dan sistematika penulisan.

#### BAB II: KAJIAN PUSTAKA

---

<sup>15</sup> Metode Analisis Bahan Hukum, diakses dari <http://repository.ub.ac.id> pada Minggu, 26 September 2021



Dalam bab ini memuat uraian mengenai pengertian perlindungan hukum, prinsip perlindungan hukum, bentuk perlindungan hukum, pengertian tindak pidana, unsur tindak pidana, sistem pemidanaan, pengertian saksi, pengertian korban, bentuk-bentuk perlindungan saksi dan korban, pengertian *cyber crime*, bentuk-bentuk *cyber crime*, serta pengertian *phishing*.

### BAB III: HASIL PENELITIAN DAN PEMBAHASAN

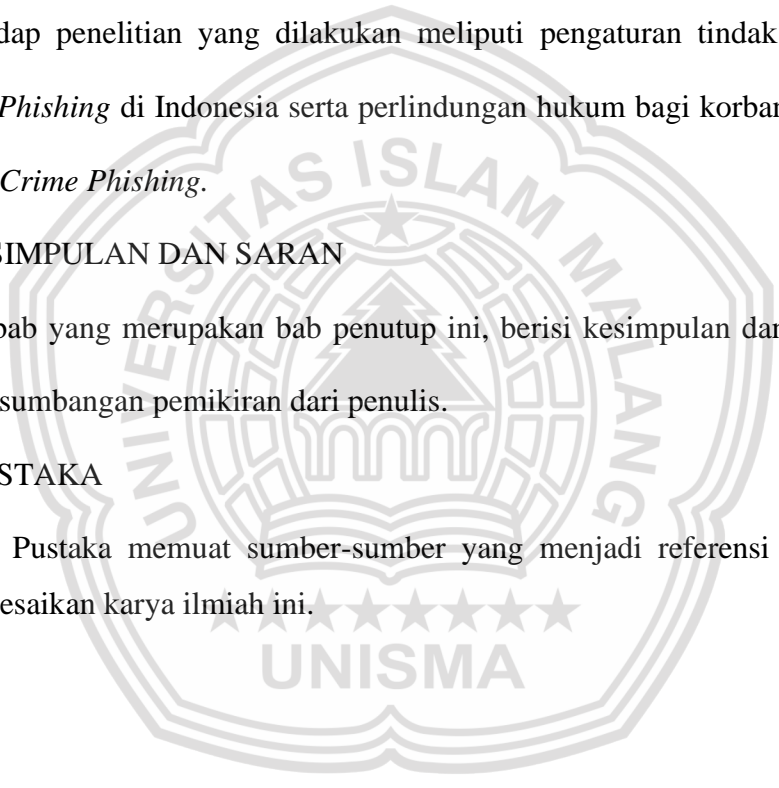
Bab ini memuat penjelasan secara luas dan terperinci sekaligus merupakan analisis terhadap penelitian yang dilakukan meliputi pengaturan tindak pidana *Cyber Crime Phishing* di Indonesia serta perlindungan hukum bagi korban tindak pidana *Cyber Crime Phishing*.

### BAB IV: KESIMPULAN DAN SARAN

Dalam bab yang merupakan bab penutup ini, berisi kesimpulan dan saran-saran sebagai sumbangan pemikiran dari penulis.

### DAFTAR PUSTAKA

Daftar Pustaka memuat sumber-sumber yang menjadi referensi penulis dalam menyelesaikan karya ilmiah ini.



## BAB IV KESIMPULAN DAN SARAN

### A. Kesimpulan

Dari penjabaran penulis diatas maka dapat ditarik kesimpulan yaitu:

#### 1. Pengaturan Tindak Pidana *Cyber Crime Phishing* di Indonesia:

- Pengaturan tindak pidana siber di Indonesia dapat dilihat dalam arti luas dan arti sempit. Secara luas, tindak pidana siber ialah semua tindak pidana yang menggunakan sarana atau dengan bantuan sistem elektronik. Itu artinya semua tindak pidana konvensional dalam Kitab Undang-Undang Hukum Pidana (KUHP) sepanjang dengan menggunakan bantuan atau sarana sistem elektronik seperti pembunuhan, perdagangan orang, dapat termasuk dalam kategori tindak pidana siber dalam arti luas.
- Dalam pengertian yang lebih sempit, pengaturan tindak pidana siber diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik..

#### 2. Perlindungan Hukum Bagi Korban Tindak Pidana *Cyber Crime Phishing*:

- Perlindungan hukum bagi korban tindak pidana *cyber crime phishing* dapat diperoleh dari pasal 378 KUHP
- Pasal 28 Ayat (1) serta Pasal 35 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dapat digunakan untuk menjerat pelaku tindak pidana *Cyber Crime Phishing* ini.

- Selain itu pelaku tindak pidana *Cyber Crime Phishing* dapat dikenakan Pasal 40 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi.

*Cyber crime* beragam bentuknya, salah satunya adalah berupa *phishing*. *Phishing* secara sederhana dapat diartikan sebagai pencurian data pribadi dengan motif memancing calon korbannya menggunakan link yang berisi gangguan. Setelah itu pelaku dapat mengakses data-data pribadi korban seperti PIN, password bahkan m-banking. Pengaruh kemajuan teknologi tidak hanya merubah kehidupan masyarakat. Namun juga bnetuk-bentuk kejahatan yang ikut berubah dan menjadi lebih canggih.

Selain kewajiban pemerintah untuk melindungi masyarakat dari dampak negatif penggunaan internet, masyarakat sendiri juga haruslah selalu bersikap waspada dan bijak dalam menggunakan internet dan bersosial media.

## B. Saran

Penulis memiliki sesuatu untuk dikatakan:

1. Saat ini kita hidup di zaman modern yang serba praktis dan canggih. Pembaruan teknologi salah satu bentuk kemajuan di zaman modern, internet adalah salah satu wujudnya. Banyak keuntungan yang didapat dari keberadaan internet. Namun selain sisi positif keberadaan internet, tentu saja terdapat hal negatif dari keberadaan internet itu sendiri. Salah satu contohnya adalah kejahatan yang menggunakan internet atau *cyber crime*. Bentuk-bentuk *cyber crime* bermacam-macam, misalnya saja *phishing*. Penulis berharap masyarakat lebih berhati-hati dan bijaksana dalam menggunakan internet. Karena *cyber crime* ini tidak mengincar siapa yang akan dijadikan korbannya. Semua orang yang menggunakan internet berpotensi untuk terkena *cyber crime*.



2. Harapan penulis agar pemerintah membuat satu aturan khusus di dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik mengenai tindak pidana *Cyber Crime Phishing* ini. Karena selama ini belum ada aturan yang mengatur secara jelas dan spesifik mengenai tindak pidana *Cyber Crime Phishing*.



## DAFTAR PUSTAKA

### Buku

- Abdul Wahid dan Mohammad Labib, 2010, *Kejahatan Mayantara (Cyber crime)*, PT. Refika Aditama, Bandung,
- Adami Chawazi, 2016, *Hukum Pidana Positif Penghinaan*, MNC, Malang
- Andi Hamzah, 1986, *Sistem Pidana dan Pemidanaan di Indonesia: dari retribusi ke reformasi*, Pradnya Paramita, Jakarta.
- Danrivanto Budhijanto, 2017, *Revolusi Cyberlaw Indonesia: Pembaruan dan Revisi UU ITE 2016*, Refika Aditama, Bandung
- Didik M. Arief Mansur & Elisatris Gultom, 2007, *Urgensi Perlindungan Korban Kejahatan Antara Norma Dan Realita*, Raja Grafindo Persada, Jakarta
- Dikdik M. Arief Mansur, Elisatris Gultom, 2005, *Cyber Law: Aspek Hukum Teknologi Informasi*, Refika Aditama, Bandung
- Ekaputra, Mohammad dan Abdul Khair, 2010, *Sistem Pidana Di Dalam KUHP Dan, Pengaturannya menurut Konsep KUHP Baru*, USU Press, Medan
- Elisabeth Nurhaini Butarbutar, 2018, *Metode Penelitian Hukum*, Refika Aditama, Bandung
- Jonaedi Efendi, Johnny Ibrahim, 2018, *Metode Penelitian Hukum Normatif dan Empiris*, Prenada Media, Jakarta
- Ekaputra, Mohammad dan Abul Khair, 2010, *Sistem Pidana Di Dalam KUHP Dan, Pengaturannya menurut Konsep KUHP Baru*, USU Press, Medan.
- Josua Sitompul, 2012, *Cyberspace Cybercrimes Cyberlaw: Tinjauan Aspek Hukum Pidana*, PT Tatanusa, Jakarta
- Lamintang, 2014, *Dasar-Dasar Hukum Pidana di Indonesia*, Sinar Grafika, Jakarta
- Moeljatno, 1983, *Asas-Asas Hukum Pidana*, Bina Aksara, Jakarta
- Moeljatno, 1985, *Azas-Azas Hukum Pidana*, Bina Aksara, Jakarta



- Moeljatno, 2000, Asas-Asas Hukum Pidana, Cetakan keenam, Rineka Cipta, Jakarta
- Muladi, 2005, Ham Dalam Persepektif Sistem Peradilan Pidana, Refika Aditama, Bandung
- Mustafa Abdullah dan Ruben Achmad, 1983, Intisari Hukum Pidana, Ghalia Indonesia, Jakarta
- Onno W Purbo dan Tony Wiharjito, 2002, Keamanan Jaringan Internet, Alex Media Komputindo, Jakarta
- Philipus M. Hadjon, 1987, Perlindungan Bagi Rakyat di Indonesia, Bina Ilmu, Surabaya
- Zaenudin Ali, 2010, Metode Penelitian Hukum, Sinar Grafika, Jakarta
- Tubagus Ronny Rahman Nitibaskara, 2001, Ketika Kejahatan Berdaulat: Sebuah Pendekatan Kriminologi, Hukum dan Sosiologi, Peradaban, Jakarta
- S.R Sianturi, 1989, Asas-Asas Hukum Pidana di Indonesia dan Penerapannya, Alumni Ahaem – Petehaem, Jakarta
- Salim HS dan Erlies Septiana Nurbaini, 2013, Penerapan Teori Hukum pada Penelitian Tesis dan Disertasi, cet. 1, PT. Rajagrafindo Persada, Jakarta
- Satcipto Rahardjo, 1983, Permasalahan Hukum di Indonesia, Alumni, Bandung
- Satjipto Raharjo, 2000, Ilmu Hukum, Citra Aditya Bakti Cetakan ke-V, Bandung
- Siswanto Sunarso, 2009, Hukum Informasi dan Transaksi Elektronik: Studi Kasus Prita Mulyasari, Rineka Cipta, Jakarta
- Soedjono Dirdjosisworo, 2008, Pengantar Ilmu Hukum, PT. Raja Grafindo Persada, Jakarta.
- Soerjono Soekanto, 1980, Pokok-Pokok Sosiologi Hukum, Rajawali Pers, Jakarta
- Soerjono Soekanto, 1984, Pengantar Penelitian Hukum, UI Press, Jakarta
- Sudarto, 1996, Kapita Selekta Hukum Pidana, Alumni, Bandung
- Sudarto, 1996, Kapita Selekta Hukum Pidana, Alumni, Bandung.
- Suratman dan Phillips Dilla, 2015, Metode Penelitian Hukum, Alfabeta Bandung, Bandung

Widodo, 2013, *Memerangi Cybercrime Karakteristik, Motivasi, dan Strategi Penanganannya dalam Prespektif Kriminologi*, Asswaja Pressindo, Yogyakarta.

### **Undang-Undang**

Kitab Undang-Undang Hukum Acara Pidana

Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 13 Tahun 2006 Tentang Perlindungan Saksi dan Korban

Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi

### **Artikel, Jurnal, Skripsi, Tesis, Disertasi, DLL**

Freddy Haris, (2004), *Cybercrime Dari Perspektif Akademis*, Lembaga Kajian Hukum dan Teknologi Fakultas Hukum Universitas Indonesia

Galuh Kartiko, 2013, *Pengaturan Terhadap Yurisdiksi Cyber crime Ditinjau dari Hukum Internasional*, Jurnal *Rechtidee*, Fakultas Hukum Universitas Trunojoyo, Vol 8 No.2 (2013)

Handrini Ardiyanti, 2014, *Cyber Security dan Tantangan Pengembangannya di Indonesia*, Jurnal *Politica* Vol. 5 No. 1 Juni 2014

Hilman Mursidi (2019), *Skripsi Fakultas Hukum Universitas Sriwijaya, Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Cyber Crime Phishing (Studi Kasus Putusan Pengadilan Negeri Medan Nomor : 3006/Pid.Sus/2017/PN.Mdn )*

Jurnal *Cendekia Hukum: Sistem Pidana dan Pemidanaan di Dalam Pembaharuan Hukum Pidana Indonesia*, Vol. 3, No 1, September 2017

Jurnal *Cendekia Hukum: Sistem Pidana dan Pemidanaan di Dalam Pembaharuan Hukum Pidana Indonesia*, Vol. 3, No 1, September 2017

Kementerian Komunikasi Informatika RI, 2011, *Buku Putih 2011 Komunikasi dan Informatika Indonesia*, PUSLITBANG APTIKA & IKIP, Jakarta

Ki Jagad Tomara (2013), *Skripsi Fakultas Hukum Universitas Brawijaya, Kajian Yuridis Pertanggungjawaban Pidana Penyedia Jasa Internet Dan Pemilik Domain Situs Phishing*

Mia Haryati Wibowo, Nur Fatimah, 2017, Ancaman *Phishing* Terhadap Pengguna Sosial Media Dalam Dunia *Cyber crime*, Jurnal of Education and Information Communication Technology, Prodi Teknologi Informasi STKIP PGRI Tulungagung, Volume 1, Nomor 1, Tahun 2017: 1 - 5

Muchsin (2003), Tesis Fakultas Hukum Universitas Sebelas Maret, Perlindungan dan Kepastian Hukum Bagi Investor di Indonesia

Sahuri Lasmadi, 2012 “Tindak Pidana Dunia Maya Dalam Perspektif Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik,” Jurnal Ilmu Hukum, Fakultas Hukum Universitas Jambi

Setiono (2004), Rule of Law (Supremasi Hukum), Tesis Fakultas Hukum Universitas Sebelas Maret, Surakarta

Yassir Arafat. 2015. Prinsip-prinsip Perlindungan Hukum yang Seimbang. Jurnal Rechtsens. Fakultas Hukum Universitas Islam Jember. Vol IV. No. 2. Edisi 2 Desember 2015

### Internet

Apa Itu *Phishing* dan Cara Menghindarinya, diakses pada Minggu 26 September 2021 dari <https://tirto.id/apa-itu-phishing-dan-bagaimana-cara-menghindarinya-ga8>

Cara Menuntut ganti Rugi Bagi Korban Tindak Pidana, diakses pada Sabtu, 27 November 2021 dari: <https://www.hukumonline.com/klinik/detail/ulasan/cl5928/ganti-rugi-dalam-kasus-pidana>

Cyber Security, diakses pada Kamis 25 November 2021 dari <https://ids.ac.id/pengertian-cyber-security/>

Data Pengguna Internet Indonesia, diakses pada Kamis, 25 November 2021 dari [https://kominform.go.id/index.php/content/detail/3415/Kominform+%3A+Pengguna+Internet+di+Indonesia+63+Juta+Orang/0/berita\\_satker](https://kominform.go.id/index.php/content/detail/3415/Kominform+%3A+Pengguna+Internet+di+Indonesia+63+Juta+Orang/0/berita_satker)

Hati-hati di Dunia Maya, Keamanan Siber Indonesia Masih Lemah, diakses pada Jumat, 26 November 2021 dari <https://biz.kompas.com/read/2017/11/30/112934928/hati-hati-di-dunia-maya-keamanan-siber-indonesia-masih-lemah>

Jerat Hukum Pelaku *Phishing* dan Modusnya, diakses pada Rabu 26 Mei 2021 dari: <https://www.hukumonline.com/klinik/detail/ulasan/cl5050/jerat-hukum-pelaku-iphishing-i-dan-modusnya/>

KBBI *Online*, diakses pada Minggu 14 November 2021 dari:  
<https://kbbi.kemdikbud.go.id/entri/korban>

Landasan Hukum Penanganan *Cyber crime* di Indonesia, diakses pada Senin 29 November 2021 dari  
<https://www.hukumonline.com/klinik/detail/ulasan/cl5960/landasan-hukum-penanganan-icybercrime-i-di-indonesia>

Malware, diakses pada Minggu 28 November 2021 dari  
<https://educsirt.kemdikbud.go.id/portal/berita/69>

Metode Analisis Bahan Hukum, diakses dari <http://repository.ub.ac.id> pada Minggu, 26 September 2021

Metode Penulisan, diakses pada Kamis 27 Mei 2021 dari:  
<http://repository.umy.ac.id/bitstream/handle/123456789/23062/BAB%20II.I.pdf?sequence=4&isAllowed=y>

Pengenalan Bahan Hukum, diakses pada Kamis 27 Mei 2021 dari  
[https://simdos.unud.ac.id/uploads/file\\_penelitian\\_1\\_dir/7847bff4505f0416fe0c446c60f7e8ac.pdf](https://simdos.unud.ac.id/uploads/file_penelitian_1_dir/7847bff4505f0416fe0c446c60f7e8ac.pdf)

Rekap Serangan Siber Januari-April 2020, diakses pada Jumat 26 November 2021 dari <https://bssn.go.id/rekap-serangan-siber-januari-april-2020/>

Serangan *Phishing* Indonesia Makin Merajalela, dikutip pada Minggu 28 November 2021 dari  
<https://www.cnbcindonesia.com/tech/20210306162132-37-228322/kasus-phishing-email-yang-serang-indonesia-makin-merajalela#>

Waspada *Phishing*, diakses pada Minggu 26 September 2021 dari:  
<https://www.uny.ac.id/waspada-phishing>