IJCLC

Indonesian Journal of Criminal Law and Criminology (IJCLC)
Volume 5, Issue 1, March 2024, 19-24

E-ISSN: 2745-7184
P-ISSN: 2745-7192

Pusat Kajian Hukum Pidana dan Kriminologi
Fakultas Hukum, Universitas Muhammadiyah Yogyakarta
E-mail: ijclc@umy.ac.id

Aspek Yuridis Kejahatan Phishing dalam Ketentuan Hukum di Indonesia

Yazid Haikal Lokapala, Fuad Januar Nurfauzi, Yeni Widowaty
Program Studi Hukum, Fakultas Hukum, Universitas Muhammadiyah Yogyakarta, Indonesia
Corrresponding author: yazid.haikal.law21@mail.umy.ac.id

Submitted: 23-01-2024; Reviewed: 28-03-2024; Revised:06-05-2024; Accepted: 08-06-2024
DOI: https://doi.org/10.18196/ijclc.v5i1.19853

Abstrak

Phishing adalah salah satu bentuk kejahatan cybercrime yang dilakukan dengan cara menipu korban untuk memberikan informasi pribadi atau rahasia melalui email, situs web, atau media sosial yang palsu. Kejahatan phishing dapat menimbulkan kerugian materiil maupun immateriil bagi korban, seperti pencurian identitas, penyalahgunaan kartu kredit, atau pencemaran nama baik. Oleh karena itu, perlu adanya upaya hukum untuk memberantas kejahatan phising dan melindungi hak-hak korban. Tulisan ini bertujuan untuk mengkaji tindak pidana kejahatan phising dalam dunia cybercrime ditinjau menurut aspek yuridis Indonesia. Metode penelitian yang digunakan adalah metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan kasus. Data yang digunakan adalah data sekunder berupa bahan hukum primer, sekunder, dan tersier. Teknik analisis data yang digunakan adalah teknik analisis kualitatif. Hasil penelitian menunjukkan bahwa phishing dalam dunia cybercrime dapat dikategorikan sebagai tindak pidana kejahatan penipuan sebagaimana diatur dalam Pasal 378 KUHP atau tindak pidana kejahatan penggelapan sebagaimana diatur dalam Pasal 372 KUHP. Phishing juga dapat dikenakan sanksi berdasarkan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), khususnya Pasal 28 ayat (1) dan Pasal 45 ayat (1) UU ITE. Masih terdapat ketidakjelasan dalam penerapan hukum terhadap kasus phishing, seperti kesulitan dalam mengidentifikasi pelaku, kurangnya koordinasi antara penegak hukum, dan rendahnya kesadaran masyarakat untuk melaporkan kasus phising. Oleh karena itu, diperlukan upaya-upaya preventif dan represif untuk mengatasi masalah tersebut, seperti meningkatkan literasi digital masyarakat, melakukan sosialisasi dan edukasi tentang bahaya phising, serta memperkuat kerjasama antara pihak-pihak terkait dalam penegakan hukum.

Keywords: efektivitas; UU ITE; cybercrime; tantangan; hambatan

Abstract

Phishing is a form of cybercrime that is committed by tricking victims into providing personal or confidential information via email, websites or fake social media. Phishing crimes can cause material and immaterial losses for victims, such as identity theft, misuse of credit cards, or defamation. Therefore, it is necessary to have legal efforts to eradicate phishing crimes and protect the rights of victims. This paper aims to examine the criminal acts of phishing crimes in the world of cybercrime in terms of Indonesian juridical aspects. The research method used is a normative legal research method with a statutory approach and a case approach. The data used is secondary data in the form of primary, secondary and tertiary legal materials. The data analysis technique used is a qualitative analysis technique. The results of the research show that the crime of phishing in the world of cybercrime can be categorized as a crime of fraud as regulated in Article 378 of the Criminal Code or an act of embezzlement as regulated in Article 372 of the Criminal Code. In addition, phishing crimes can also be subject to sanctions based on Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), specifically Article 28 paragraph (1) and Article 45 paragraph (1) of the ITE Law. However, in practice, there are still obstacles in law enforcement against phishing crimes, such as difficulties in identifying perpetrators, lack of coordination between law enforcement, and low public awareness to report phishing cases. Therefore, preventive and repressive efforts are needed to overcome this problem, such as increasing people's digital literacy, conducting socialization and education about the dangers of phishing, and strengthening cooperation between related parties in law enforcement.

Keywords: effectiveness; ITE law; cybercrime; challenges; obstacles

I. Pendahuluan

Saat ini teknologi informasi dan komunikasi berkembang dengan sangat strategis, menciptakan dunia tanpa batas, jarak, ruang, dan waktu sehingga mampu mengubah cara hidup seseorang serta tatanan

kehidupan baru, yang mendorong perubahan sosial, ekonomi, budaya, dan pertahanan keamanan.[1] Perkembangan teknologi juga memberikan peluang terhadap terjadinya tindakan kejahatan yang semakin canggih dan kompleks. Salah satu bentuk kejahatan yang muncul adalah kejahatan *phishing.*

Phishing merupakan tindakan penipuan yang dilakukan secara daring dengan tujuan memperoleh informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi keuangan lainnya dari korban dengan mencuri identitas, merampas dana, atau merusak reputasi. *Phishing* menjadi kejahatan yang perlu mendapatkan perhatian serius karena mengancam keamanan data pribadi, kenyamanan bertransaksi daring, serta integritas ekonomi negara. Pelaku *phishing* umumnya menyamar sebagai entitas yang sah, seperti perusahaan atau lembaga keuangan terkemuka, untuk memancing korban agar memberikan informasi pribadi mereka dengan dalih palsu. Modus yang dilakukan dengan memanfaatkan teknik sosial, manipulasi, dan teknologi sehingga dapat merugikan individu dan organisasi.[2]

Pelaku *phishing* dapat menggunakan cara melalui *email phishing* untuk mendapatkan data pribadi dengan menyamar sebagai orang atau organisasi yang berwenang melalui *email*. Mengutip data yang bersumber dari Badan Siber dan Sandi Negara (BSSN) terdapat 164.131 kasus *email phishing* yang terjadi di Indonesia pada tahun 2022. Kasus *email phishing* yang paling banyak berasal dari *email* pribadi (59.210 kasus), dengan 52.744 kasus berasal dari *email* grup, dan 52.177 kasus berasal dari *email* lainnya. Adapun, 93.897 kasus *email phishing* terjadi selama jam kerja, yaitu dari pukul 09.00 hingga 17.00, 70.234 kasus lainnya terjadi di luar jam kerja, yaitu dari pukul 17.00 hingga 09.00.[3] Contoh kasus *phishing* lainnya terjadi di Malang, Jawa Timur yang menyebabkan korban mengalami kerugian lebih dari satu miliar rupiah. Korban adalah pengusaha aksesori kendaraan Silvia YAP yang mendapatkan link undangan palsu melalui *whats app.* Link tersebut ternyata menyebabkan pembobolan terhadap beberapa aplikasi *mobile banking* milik korban[4]

Perkembangan teknologi dan modus operandi pelaku kejahatan yang terus berubah, sehingga diperlukan pemahaman yang mendalam mengenai aspek yuridis terkait dengan *phishing* dalam ketentuan hukum di Indonesia. Aspek yuridis akan digunakan untuk menganalisis ketentuan hukum yang ada, mekanisme penanganan kasus, serta kendala-kendala yang dihadapi oleh aparat penegak hukum dan saran perbaikan dalam penanganan kejahatan *phishing*. Artikel yang disusun diharapkan dapat memberikan kontribusi bagi upaya penguatan sistem hukum dan penegakan hukum dalam menghadapi tantangan dunia *cyber crime* khususnya kejahatan *phishing* di Indonesia dan membahas lebih lanjut mengenai efektifivitas hukum Indonesia dalam menanggulangi kasus *phishing* yang terjadi serta apa saja hambatan dan tantangan apa yang ditemukan dalam menangani kejahatan *phishing*.

II. Metode Penelitian

Penelitian disusun menggunakan penelitian hukum normatif atau penelitian kepustakaan yang dilakukan terhadap bahan pustaka atau data sekunder.[5] Kajian hukum normatif disebut juga kajian dokumen atau kajian kepustakaan yang terbatas pada undang-undang tertulis atau bahan hukum pelengkap lainnya.[6] Pendekatan penelitian yang digunakan yaitu pendekatan undang-undang dan

[1] Siswanto Sunarso, Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari, PT. Rineka Cipta, Jakarta, 2009, hlm. 39.

[2] Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber," Jurnal Saintkom, Vol. 13, No. 3, 2014, hlm. 211.

[3] Sarnita Sadya, *Ada 164.131 Kasus Email Phising di Indonesia pada 2022*, https://dataindonesia.id/internet/detail/ada-164131-kasus-email-phising-di-indonesia-pada-2022.

[4] Aditya Priyatna Darmawan, *Kronologi Wanita di Malang Kehilangan Tabungan Rp 1,4 Miliar Usai Klik Undangan Pernikahan di WhatsApp*, https://www.kompas.com/tren/read/2023/07/07/131500065/kronologi-wanita-di-malang-kehilangan-tabungan-rp-1-4-miliar-usai-klik?page=all.

[5] Suratman dan Phillips Dilla, 2015, Metode Penelitian Hukum, Alfabeta Bandung, Bandung hlm 65

[6] Elisabeth Nurhaini Butarbutar, 2018, Metode Penelitian Hukum, Refika Aditama, Bandung, hlm 84

pendekatan konseptual. Bahan hukum yang berhasil ditemukan akan diolah dan dianalisis secara komprehensif melalui metode destruktif dengan memaparkan secara terperinci dan tepat berkaitan dengan fenomena *phishing* serta secara kualitatif akan dipaparkan dalam hasil penulisan yang sudah disistematisasikan dengan kajian dari teori-teori hukum dan hukum positif yang digunakan.

III. Hasil dan Pembahasan

3.1. Efektivitas Sistem Hukum Indonesia dalam Menangani *Phishing* sebagai Bentuk *Cybercrime*

Phishing merupakan tindakan penipuan yang dilakukan secara daring untuk memperoleh informasi pribadi atau rahasia dari korban yang dapat menimbulkan kerugian materiil maupun immateriil bagi korban, seperti pencurian identitas, penyalahgunaan kartu kredit, atau pencemaran nama baik. *Phishing* dilakukan dengan berbagai cara seperti mengirimkan email, situs web, atau media sosial yang palsu yang mengatasnamakan lembaga resmi atau terpercaya. *Phishing* menjadi kejahatan yang perlu mendapatkan perhatian serius karena tidak hanya mengancam keamanan data pribadi, kenyamanan bertransaksi daring tetapi juga dapat menganggu integritas ekonomi negara.

Kejahatan *phishing* merupakan perbuatan yang dapat dikategorikan sebagai tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP atau tindak pidana penggelapan sebagaimana diatur dalam Pasal 372 KUHP. Secara khusus ketentuan terkait kejahatan *phishing* diatur sebagai berikut:

a. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang merupakan payung hukum utama dalam bidang *cyber law* di Indonesia. UU ITE mengatur berbagai aspek hukum terkait dengan informasi dan transaksi elektronik, termasuk tindak pidana siber. Beberapa pasal yang berkaitan dengan *phishing* adalah:
    1) Pasal 28 ayat (1) berkaitan dengan penyebaran informasi dan dokumen elektronik yang mengandung informasi palsu yang dapat merugikan pelanggan saat melakukan transaksi elektronik.[7]
    2) Pasal 30 ayat (1) tentang akses ilegal terhadap sistem elektronik milik orang lain atau masyarakat umum tanpa izin atau hak.
    3) Pasal 31 ayat (1) Untuk mengubah, menambah, mengurangi, mengirim, merusak, menghilangkan, memindahkan, atau menyembunyikan dokumen elektronik dan informasi elektronik milik orang lain atau masyarakat umum tanpa hak.
    4) Pasal 32 ayat (1) tentang pemalsuan dokumen dan/atau informasi elektronik dengan kehati-hatian yang memadai agar dapat dianggap sebagai dokumen dan/atau informasi elektronik asli.
    5) Pasal 35 ayat (1) tentang penggunaan informasi elektronik dan/atau dokumen elektronik palsu sebagai alat bukti dalam transaksi elektronik.
    6) Pasal 36 ayat (1) tentang manipulasi terhadap sistem elektronik milik orang lain atau masyarakat umum dengan maksud untuk mendapatkan keuntungan bagi diri sendiri atau orang lain secara tidak sah.[8]
b. Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE Perubahan), yang merupakan revisi dari UU ITE sebelumnya. UU ITE Perubahan menambahkan beberapa pasal baru yang berkaitan dengan *phishing,* yaitu:
    1) Pasal 28A tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung ancaman kekerasan atau menakut-nakuti yang dapat menimbulkan rasa takut atau keresahan pada masyarakat umum.[9]
    2) Pasal 28B tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung penghinaan dan/atau pencemaran nama baik.

[7] Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).
[8] Ibid
[9] Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE Perubahan).

3) Pasal 28C tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung fitnah atau pemerasan.
4) Pasal 28D tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung hasutan untuk melakukan tindak pidana.
5) Pasal 28E tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung kebencian atau permusuhan terhadap suku, agama, ras, dan antargolongan (SARA).
6) Pasal 28F tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung pornografi atau perbuatan asusila.
7) Pasal 28G tentang penyebaran informasi elektronik dan/atau dokumen elektronik yang mengandung perjudian.[10]

Ketentuan kejahatan *phishing* yang sebelumnya diatur dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik kemudian diubah menjadi Undang-undang Nomor 19 Tahun 2016 tentang Revisi Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang masih berlaku hingga saat ini. Ketentuan tersebut mengatur tentang pasal-pasal yang berkaitan dan dapat diterapkan untuk kejahatan *phishing* seperti penipuan elektronik, pemalsuan identitas, dan pencurian data pribadi berikut dengan ketentuan sanksinya. Pengaturan tentang kejahatan *phishing* masih menimbulkan perdebatan terutama berkaitan dengan efektivitas hukuman dan sanksi terhadap pelaku tindak pidana *phishing* yang selama ini diterapkan. Beberapa berpendapat mengatakan bahwa hukuman yang lebih tegas diperlukan untuk memberikan efek jera, sementara yang lain menganggap bahwa pendekatan edukatif dan rehabilitatif juga penting untuk mengubah pelaku.

Penegakan hukum terhadap kejahatan *phising* sudah dimulai melalui aspek kultural agar terdapat kesadaran dan partisipasi masyarakat dalam mencegah dan menangani kejahatan *phishing*. Berikut ini adalah aspek kultural yang dapat dilakukan melalui beberapa program yang bertujuan untuk meningkatkan literasi dan edukasi siber bagi masyarakat, seperti:

1) Gerakan Nasional Siber Bersih (Gernas Cinta Siber) merupakan gerakan bersama antara pemerintah, swasta, akademisi, dan masyarakat sipil untuk menciptakan lingkungan siber yang bersih, sehat, dan aman di Indonesia.
2) Indonesia *Cyber Security* Forum (ICSF) merupakan forum yang menghimpun berbagai pemangku kepentingan di bidang keamanan siber untuk berbagi informasi, pengetahuan, dan pengalaman dalam menghadapi tantangan siber di Indonesia.
3) *Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII) merupakan tim tanggap insiden keamanan siber yang berfokus pada infrastruktur internet di Indonesia, termasuk memberikan layanan pemberitahuan, peringatan, dan rekomendasi terkait dengan ancaman siber.
4) Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), yang merupakan asosiasi yang mewadahi para penyelenggara jasa internet di Indonesia, termasuk memberikan edukasi dan sosialisasi mengenai etika dan tata cara berinternet yang baik dan benar.

Penegakan hukum *phishing* masih menimbulkan hambatan dan tantangan terutama dalam aspek stuktural. Pertama, disebabkan karena belum adanya koordinasi atau sinergi yang optimal antara lembaga-lembaga penegak hukum dalam menangani kejahatan *phishing* yang melibatkan aparat kepolisian, Ditjen Pajak, dan lembaga terkait lainnya sehingga dapat menyebabkan tumpang tindih atau konflik kewenangan antara lembaga-lembaga tersebut. Kedua, belum adanya standar atau pedoman operasional yang seragam dan terintegrasi dalam menangani kejahatan *phishing* sehingga menyebabkan inkonsistensi atau ketidakefisienan dalam proses penegakan hukumnya. Ketiga, belum adanya sumber daya manusia (SDM) yang memadai dan kompeten dalam menangani kejahatan *phishing* sehingga menyebabkan kesulitan atau keterbatasan dalam melakukan penyelidikan, penyidikan, penuntutan, atau pemeriksaan terhadap tindak pidana *phishing.* Keempat, belum adanya fasilitas atau peralatan yang memadai dan canggih dalam menangani kejahatan *phishing* sehingga menyebabkan kesulitan atau keterbatasan dalam melakukan pengumpulan, pengolahan, penyimpanan, atau penganalisisan bukti-bukti elektronik terkait dengan kejahatan *phishing*.

Dua pendekatan dalam penegakan hukum *phishing* baik yang berfokus pada aspek struktural maupun kultural masih ditemukan beberapa kelemahan, kekurangan, tantangan, dan hambatan yang perlu

[10] Ibid

diperbaiki dan ditingkatkan. Penegakan hukum dalam aspek kultural dalam praktiknya tidak sejalan dengan penegakan hukum dalam aspek struktural sehingga masih ditemukan kendala dan hambatan dalam menanggulangi kejahatan *phishing*. Pendekatan secara integral melalui upaya preventif dan represif sangat diperlukan untuk mengatasi kejahatan *phishing*. Upaya yang dapat dilakukan antara lain meningkatkan literasi digital masyarakat, melakukan sosialisasi dan edukasi tentang bahaya *phishing*, memperkuat kerjasama antara pihak-pihak terkait dalam penegakan hukum serta perbaikan dan penyempurnaan dari aspek regulasi hukum yang mengatur tentang kejahatan *phishing* agar dapat memberikan perlindungan hukum yang lebih efektif dan efisien bagi korban.

3.2. Tantangan dan Hambatan dalam Menangani Kejahatan *Phishing*

Phishing adalah praktik penipuan di mana pelaku mencoba mendapatkan informasi pribadi, seperti kata sandi dan informasi keuangan, dengan menyamar sebagai individu terpercaya melalui pesan elektronik atau situs web palsu. Berikut adalah beberapa tantangan dalam menangani kejahatan *phishing*:[11]

Pertama, kejahatan *phishing* terjadi karena kurangnya kesadaran dan pengetahuan masyarakat untuk menghadapi dan melindungi diri sehingga membuat masyarakat rentan menjadi korban. Kedua, kejahatan *phishing* terjadi karena keterbatasan sumber daya manusia yang professional dan memiliki kualifikasi khusus untuk mengidentifikasi kejahatan *phishing.* Ketiga, kejahatan *phishing* juga terjadi karena keterbatasan teknologi yang dimiliki yang memudahkan pelaku melakukan kejahatan dengan teknik kamuflase yang canggih. Keempat, kejahatan *phishing* terjadi apabila melibatkan lebih dari satu yurisdiksi negara yang berbeda yang dapat mempersulit proses penegakan hukumnya karena menjadi sangat rumit dan kompleks misalnya dalam pengumpulan bukti digital. Kelima, kejahatan *phishing* terjadi karena ketidakpastian hukum dalam penerapan undang-undang yang digunakan apalagi jika kejahatan tersebut dilakukan dengan melibatkan yurisdiksi negara lain sehingga membutuhkan adanya kerjasama internasional yang solid melalui undang-undang khusus untuk menanggulangi kejahatan *phishing.*

Tantangan dalam menangani kejahatan *phishing* perlu diatasi dengan baik dimulai dengan meningkatkan kesadaran masyarakat mengenai keamanan siber, membekali lembaga penegak hukum dengan keterampilan dan alat yang diperlukan, memperkuat kerja sama internasional dalam memerangi kejahatan siber lintas batas negara, dan mempertimbangkan untuk memperbaiki undang-undang yang ada agar dapat memberantasnya secara lebih efektif.[12] Berikut ini adalah hambatan yang biasanya dihadapi oleh negara dalam menanggulangi kejahatan *phishing.* Pertama, belum banyak korban yang berani melaporkan kejahatan *phishing* yang terjadi karena malu dan tidak tahu prosedur hukumnya. Kedua, kesulitan dalam penegakan hukum karena kurangnya bukti dan keterbatasan sumber daya aparat penegak hukum baik dalam kemampuan professional maupun dalam kemampuan penggunaan teknologi. Ketiga, perubahan modus kejahatan *phishing* seiring dengan perkembangan dan kemajuan teknologi.[13]

IV. Simpulan

Kejahatan *phishing* dapat dikategorikan sebagai tindak pidana penipuan sebagaimana diatur dalam Pasal 378 KUHP atau tindak pidana penggelapan sebagaimana diatur dalam Pasal 372 KUHP dan diatur secara khusus dalam Pasal 28 ayat (1) dan Pasal 45 ayat (1) UU ITE. Penegakan hukum terhadap kejahatan *phishing* masih menimbulkan hambatan dan tantangan terutama dalam aspek stuktural dan aspek kultural seperti masih terdapat ketidakjelasan dalam penerapan hukum, kesulitan dalam mengidentifikasi pelaku, kurangnya koordinasi antara penegak hukum, dan rendahnya kesadaran masyarakat untuk melaporkan kasus *phishing.* Hambatan dan tantangan tersebut perlu diatasi melalui pendekatan secara integral menggunakan upaya preventif dan represif untuk mengatasi kejahatan *phishing* sehingga penegakan hukum terhadap kejahatan *phishing* menjadi lebih efektif. Upaya tersebut dilakukan dengan meningkatkan literasi digital masyarakat, melakukan sosialisasi dan edukasi tentang bahaya *phishing*, memperkuat kerjasama antara pihak-pihak terkait dalam penegakan hukum serta perbaikan dan penyempurnaan dari aspek regulasi hukum yang mengatur tentang kejahatan *phishing* agar dapat memberikan perlindungan hukum yang lebih efektif dan efisien bagi korban.

[11] Fiorida Mathilda, "Cyber Crime dalam Sistem Hukum Indonesia," Sigma-Mu4, no. 2 (September 2012): 36

[12] Maskun, 2013, Kejahatan Siber(Cyber Crime), Jakarta: Kencana

[13] Tanthawi, Dahlan, Suhaimi. Perlindungan Korban Tindak Pidana Cyber Crime dalam Sistem Hukum Pidana Indonesia, Jurnal Ilmu Hukum Vol. 2 No. 1, 2014. Hlm. 38.

Daftar Pustaka.

Undang-Undang:

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE Perubahan).

Buku:

Elisabeth Nurhaini Butarbutar, 2018, Metode Penelitian Hukum, Refika Aditama, Bandung

Maskun, 2013, Kejahatan Siber (*Cyber Crime*), Kencana, Jakarta

Siswanto Sunarso, 2009, Hukum Informasi dan Transaksi Elektronik, Studi Kasus Prita Mulyasari, Rineka Cipta, Jakarta

Suratman dan Phillips Dilla, 2015, Metode Penelitian Hukum, Alfabeta Bandung, Bandung

Jurnal:

Dian Rachmawati, "Phising Sebagai Salah Satu Bentuk Ancaman dalam Dunia Cyber," Jurnal Saintkom, Vol. 13, No. 3, 2014

Fiorida Mathilda, "Cyber Crime dalam Sistem Hukum Indonesia," Sigma-Mu4, no. 2 (September 2012)

Tanthawi, Dahlan, Suhaimi. Perlindungan Korban Tindak Pidana *Cyber Crime* dalam Sistem Hukum Pidana Indonesia, Jurnal Ilmu Hukum Vol. 2 No. 1, 2014.

Internet:

Aditya Priyatna Darmawan, *Kronologi Wanita di Malang Kehilangan Tabungan Rp 1,4 Miliar Usai Klik Undangan Pernikahan di WhatsApp*, https://www.kompas.com/tren/read/2023/07/07/131500065/kronologi-wanita-di-malang-kehilangan-tabungan-rp-1-4-miliar-usai-klik?page=all.

Sarnita Sadya, Ada 164.131 Kasus Email Phising di Indonesia pada 2022, https://dataindonesia.id/internet/detail/ada-164131-kasus-email-phising-di-indonesia-pada-2022.