Fairness and Justice: Jurnal Ilmiah Ilmu Hukum
p-ISSN: 1858-0106 e-ISSN: 2502-3926
Volume 20 Nomor 2 November, 2022
http://jurnal.unmuhjember.ac.id/index.php/FAJ

Typosquatting: Ancaman dan Dampaknya dalam Kejahatan Teknologi Informasi

Muhammad Asrul Maulana[1], Safia Adysti Mutiara Aaliyah Sulaiman[2]

[1]Fakultas Bisnis Hukum dan Ilmu Sosial Universitas Muhammadiyah Sidoarjo
E-mail: asrulnaa7@gmail.com
[2]Fakultas Bisnis Hukum dan Ilmu Sosial Universitas Muhammadiyah Sidoarjo
E-mail: adistysulaiman89@gmail.com

Abstract

This study aims to analyze and understand the impact of typos on internet users and see the legal sanctions that can be imposed on the perpetrators. The results of the study show that typos can be detrimental to internet users with the potential for loss of personal information, financial losses, and damage to devices. Typical errors can be subject to severe legal penalties, including fines and prison terms, as well as freezing or deletion of their websites. Therefore, internet users need to raise awareness, be careful when entering URLs, and use security measures such as firewalls and antiviruses to protect themselves from typos.
Keywords: typosquatting, Implication Law.

Abstrak

Penelitian ini bertujuan untuk menganalisis dan memahami dampak typosquatting terhadap pengguna internet serta melihat sanksi hukum yang dapat dikenakan kepada pelakunya. Hasil penelitian menunjukkan bahwa typosquatting dapat merugikan pengguna internet dengan potensi kehilangan informasi pribadi, kerugian finansial, dan kerusakan perangkat. Pelaku typosquatting dapat dikenakan sanksi hukum berat, termasuk denda dan hukuman penjara, serta pembekuan atau penghapusan situs web mereka. Oleh karena itu, pengguna internet perlu meningkatkan kesadaran, berhati-hati dalam memasukkan URL, dan menggunakan langkah-langkah keamanan seperti firewall dan antivirus guna melindungi diri dari typosquatting.
Kata Kunci: Kesalahan Penulisan, Implikasi Hukum.

1. Pendahuluan

Definisi typosquatting adalah praktik membeli domain yang mirip dengan domain populer dengan tujuan untuk menyalahgunakan traffic yang salah sasaran atau menyimpan konten yang tidak sesuai dengan yang diharapkan oleh pengguna. Contoh typosquatting adalah ketika seseorang membeli domain "googel.com" yang mirip dengan domain "google.com" dengan tujuan untuk mengarahkan pengguna yang salah mengetik ke situs yang tidak sesuai dengan yang diharapkan. Tujuan typosquatting biasanya adalah untuk mengarahkan traffic ke situs yang tidak sesuai dengan yang diharapkan atau untuk menyimpan konten yang tidak sesuai dengan yang diharapkan oleh pengguna, seperti iklan atau malware [1].

[1] White dan Cornu, "Visitors and Residents: A new typology for online engagement."

Situs web terkenal yang untuk memikat pengunjung yang tidak menaruh curiga ke situs web alternatif, biasanya untuk tujuan jahat. Typostquatting dapat ditindaklanjuti berdasarkan Anticybersquatting Consumer Protection Act ("ACPA"), dan korban berhak atas ganti rugi menurut undang-undang hingga $100.000 per nama domain. Postquatters Ty dapat mengambil keuntungan dari iniTyposquatting adalah bentuk kejahatan dunia maya di mana peretas mendaftarkan domain dengan nama situs web terkenal yang sengaja salah eja untuk memikat pengunjung yang tidak menaruh curiga ke situs web alternatif, biasanya untuk tujuan jahat. Typosquatting dapat ditindaklanjuti berdasarkan Anticybersquatting Consumer Protection Act ("ACPA"), dan korban berhak atas ganti rugi menurut undang-undang hingga $100.000 per nama domain. Typosquatters dapat memperoleh keuntungan dari perilaku ini dalam berbagai cara, seperti menyediakan pop-up untuk pengiklan pihak ketiga, menangkap informasi pembayaran yang curang, atau bahkan menjual domain kepada pemilik [2].

Typosquatting bukan satu-satunya cara scammers dapat mengelabui orang agar memberikan informasi pribadi atau mengunjungi situs web yang dipenuhi malware. Combosquatting melibatkan penambahan kata baru ke nama domain yang sudah ada untuk membuat situs baru, sedangkan jenis typosquatting lainnya termasuk salah eja yang umum, menambahkan 's' atau titik ekstra.

Cara kerja typosquatting meliputi. Mencari domain yang mirip dengan domain populer: Typosquatters biasanya mencari domain yang mirip dengan domain populer dengan menggunakan tanda baca yang salah, spelling yang salah, atau kombinasi karakter yang mirip dengan domain asli. Mereka kemudian akan membeli domain tersebut dengan tujuan untuk menyalahgunakan traffic yang salah sasaran [3].

Menyalahgunakan traffic yang salah sasaran: Setelah membeli domain yang mirip dengan domain populer, typosquatters akan mengarahkan traffic yang salah sasaran ke situs yang tidak sesuai dengan yang diharapkan. Ini bisa dilakukan dengan menyimpan konten yang tidak sesuai dengan yang diharapkan oleh pengguna atau dengan menampilkan iklan yang tidak sesuai dengan yang diharapkan.

Menyimpan konten yang tidak sesuai dengan yang diharapkan oleh pengguna: Typosquatters juga dapat menyimpan konten yang tidak sesuai dengan yang diharapkan oleh pengguna di situs yang mereka miliki. Ini bisa berupa iklan yang tidak sesuai dengan yang diharapkan, malware, atau konten yang tidak sesuai dengan yang diharapkan. Typosquatting dapat menyebabkan beberapa dampak negatif bagi pengguna dan pemilik domain asli. Dampak yang mungkin terjadi adalah kerugian bagi pengguna yang terkena typosquatting: Pengguna yang salah mengetik alamat web atau yang tidak sengaja mengklik tautan yang salah sasaran dapat terkena typosquatting. Mereka kemudian akan diarahkan ke situs yang tidak

[2] Bakhareva, "Objects of intellectual property rights: general terms of protection."
[3] Rong, "Discuss of Typological of the Intellectual Property Crime."

sesuai dengan yang diharapkan, yang dapat menyebabkan kerugian bagi pengguna tersebut. Contohnya, pengguna dapat mengalami kehilangan uang atau kehilangan data pribadi jika situs yang diakses tidak aman [4].

Kerugian bagi perusahaan atau individu yang domain aslinya disalahgunakan: Typosquatting juga dapat menyebabkan kerugian bagi perusahaan atau individu yang domain aslinya disalahgunakan. Ini bisa terjadi karena traffic yang seharusnya akan mengunjungi situs asli tidak sampai ke tujuan. Hal ini dapat menjadi pemicu berpotensi terciptanya Kejahatan Teknologi Informasi

2. Metode

Menggunakan metode normatif dengan melakukan analisis terhadap peraturan perundang-undangan yang berlaku di negara yang bersangkutan terkait dengan transaksi keuangan dan teknologi blockchain. Ini melibatkan studi dan penafsiran terhadap undang-undang, peraturan pemerintah, perjanjian internasional, dan kebijakan terkait. Serta menggunakan pendekatan studi kasus dengan mengidentifikasi dan menganalisis kasus-kasus yang terkait dengan penggunaan teknologi blockchain dalam transaksi keuangan. Menelaah putusan pengadilan, arbitrase, atau proses hukum lainnya yang berkaitan dengan isu hukum yang muncul dalam konteks ini. Analisis ini akan membantu memahami bagaimana hukum diterapkan dalam situasi nyata dan bagaimana keputusan-keputusan hukum tersebut dapat mempengaruhi penggunaan teknologi blockchain dalam transaksi keuangan.

3. Hasil dan Pembahasan

Typosquatting adalah salah satu jenis kejahatan teknologi informasi yang sering terjadi di dunia maya. Typosquatting merupakan sebuah tindakan yang dilakukan oleh seorang pelaku dengan memanfaatkan kesalahan pengetikan yang dilakukan oleh orang lain.

Cara kerja dari typosquatting ini adalah dengan membuat sebuah website yang terlihat mirip dengan website asli, namun dengan sedikit perbedaan pada alamat URL-nya. Pelaku typosquatting akan memanfaatkan kesalahan pengetikan yang dilakukan oleh orang lain, sehingga orang tersebut akan ter redirect ke website palsu yang dibuat oleh pelaku [5].

Biasanya, pelaku typosquatting akan menggunakan website palsu tersebut untuk mengumpulkan informasi pribadi dari pengunjung website yang tidak sengaja

[4] Peytchev dan Crawford, "A Typology of Real-Time Validations in Web-Based Surveys."
[5] Peytchev Dan Crawford.

terredirect ke sana. Informasi pribadi yang biasanya dikumpulkan oleh pelaku typosquatting adalah seperti nama, alamat email, dan nomor telepon [6].

Typosquatting ini merupakan salah satu jenis kejahatan teknologi informasi yang sangat merugikan bagi para pengguna internet. Selain mengumpulkan informasi pribadi, pelaku typosquatting juga dapat menggunakan website palsu tersebut untuk melakukan phishing atau menyebarkan malware. Oleh karena itu, penting sekali bagi para pengguna internet untuk selalu waspada dan memastikan bahwa mereka tidak salah memasukkan alamat URL saat ingin mengakses sebuah website [7].

Typosquatting adalah salah satu jenis kejahatan teknologi informasi yang dilakukan dengan cara memanfaatkan kesalahan pengetikan yang dilakukan oleh orang lain. Untuk melakukan typosquatting, pelaku biasanya melakukan beberapa tahap seperti yang Anda sebutkan di atas, yaitu:

Mencari domain yang mirip dengan domain populer: Pelaku akan mencari dan mendaftarkan sebuah domain yang mirip dengan domain populer, namun dengan sedikit perbedaan pada alamat URL-nya. Misalnya, domain populer adalah "www.example.com", maka pelaku akan mendaftarkan domain yang mirip seperti "www.examp1e.com" atau "www.exampl3.com".

Menyalahgunakan traffic yang salah sasaran: Setelah memiliki domain yang mirip dengan domain populer, pelaku akan menunggu orang lain yang salah mengetik alamat URL domain populer tersebut. Ketika orang tersebut salah mengetik alamat URL dan terredirect ke domain palsu yang dibuat oleh pelaku, maka pelaku akan menyalahgunakan traffic yang salah sasaran tersebut.

Menyimpan konten yang tidak sesuai dengan yang diharapkan oleh pengguna: Pelaku typosquatting biasanya akan menyimpan konten yang tidak sesuai dengan yang diharapkan oleh pengguna di website palsu yang dibuatnya. Konten tersebut bisa berupa iklan yang mengganggu, atau bahkan konten yang tidak sesuai dengan yang diharapkan oleh pengguna [8].

Typosquatting merupakan salah satu jenis kejahatan teknologi informasi yang sangat merugikan bagi para pengguna internet. Selain menyalahgunakan traffic yang salah sasaran, pelaku typosquatting juga dapat menggunakan website palsu tersebut untuk melakukan phishing atau menyebarkan malware.

Phishing adalah sebuah tindakan yang dilakukan oleh pelaku dengan mengirimkan email atau pesan yang terlihat seperti datang dari sebuah perusahaan

[6] Jubaedi Dan Irawan, "Perancangan Program Acara TeIEvisi Menggunakan Teknik Editing Kinetic Typography."
[7] Dam, Klausner, dan Schrittwieser, "Typosquatting for Fun and Profit: Cross-Country Analysis of Pop-Up Scam."
[8] Adebayo dkk., "A Gamified Technique to Improve Users' Phishing and Typosquatting Awareness."

atau organisasi terpercaya, namun sebenarnya dikirimkan oleh pelaku untuk menipu pengguna dan mengumpulkan informasi pribadi dari mereka.

Malware adalah sebuah software yang tidak diinginkan yang dapat menyebabkan kerusakan pada komputer atau perangkat lainnya. Malware dapat berupa virus, trojan, worm, atau bahkan adware yang dapat menyebar dengan cepat ke komputer lainnya.

Oleh karena itu, penting sekali bagi para pengguna internet untuk selalu waspada dan memastikan bahwa mereka tidak salah memasukkan alamat URL saat ingin mengakses sebuah website. Selain itu, pengguna juga harus selalu menjaga keamanan informasi pribadi mereka dan tidak memberikan informasi pribadi kepada pihak yang tidak dapat dipercaya.

3.1 Dampak Typosquatting

Dampak dari typosquatting bisa sangat merugikan bagi para pengguna internet. Beberapa dampak yang dapat ditimbulkan oleh typosquatting adalah:

Kehilangan informasi pribadi: Pelaku typosquatting dapat mengumpulkan informasi pribadi dari para pengunjung website yang tidak sengaja terredirect ke website palsu yang dibuatnya. Informasi pribadi yang dikumpulkan oleh pelaku bisa berupa nama, alamat email, nomor telepon, dan informasi lainnya yang bisa digunakan oleh pelaku untuk kejahatan lainnya [9].

Kehilangan uang: Pelaku typosquatting juga dapat menggunakan website palsu tersebut untuk melakukan phishing, dimana pelaku akan mengirimkan email atau pesan yang terlihat seperti datang dari perusahaan atau organisasi terpercaya, namun sebenarnya dikirimkan oleh pelaku untuk menipu pengguna dan mengumpulkan informasi pribadi dari mereka. Jika pengguna terkecoh dan memberikan informasi pribadi atau bahkan uang kepada pelaku, maka pengguna tersebut bisa kehilangan uangnya.

Kerusakan pada perangkat: Pelaku typosquatting juga dapat menyebarkan malware melalui website palsu yang dibuatnya. Jika pengguna terinfeksi oleh malware tersebut, maka dapat menyebabkan kerusakan pada perangkat yang digunakan, seperti komputer, smartphone, atau perangkat lainnya.

Kerugian reputasi: Selain kehilangan informasi pribadi dan uang, pengguna juga bisa kehilangan reputasinya jika informasi pribadi yang hilang tersebut digunakan oleh pelaku untuk kejahatan lainnya. Misalnya, jika informasi pribadi yang hilang tersebut digunakan oleh pelaku untuk melakukan spam atau menyebarkan informasi yang tidak benar, maka reputasi pengguna bisa tercemar [10].

[9] Banerjee, Rahman, dan Faloutsos, "SUT: Quantifying and mitigating URL typosquatting."
[10] Dewi, "Kejahatan Teknologi Hacking Paypal."

Oleh karena itu, penting sekali bagi para pengguna internet untuk selalu waspada dan memastikan bahwa mereka tidak salah memasukkan alamat URL saat ingin mengakses sebuah website.

3.2 Akibat Hukum Pelaku Typosquatting

Typosquatting merupakan salah satu jenis kejahatan teknologi informasi yang dapat merugikan para pengguna internet. Oleh karena itu, pelaku typosquatting biasanya akan dikenakan sanksi hukum yang cukup berat.

Di beberapa negara, pelaku typosquatting dapat dikenakan sanksi hukum berupa denda atau hukuman penjara. Selain itu, pelaku juga dapat dikenakan sanksi administratif berupa pembekuan atau penghapusan website yang dibuatnya, serta pembatalan registrasi domain yang digunakan untuk melakukan typosquatting.

Selain sanksi hukum, pelaku typosquatting juga dapat dikenakan sanksi dari lembaga-lembaga yang bertanggung jawab terhadap keamanan internet, seperti Internet Corporation for Assigned Names and Numbers (ICANN) atau organisasi lainnya yang bertugas mengatur penggunaan domain di internet [11].

Untuk menghindari terkena sanksi hukum atau sanksi dari lembaga terkait, penting bagi para pengguna internet untuk selalu waspada dan memastikan bahwa mereka tidak salah memasukkan alamat URL saat ingin mengakses sebuah website. Selain itu, pengguna juga harus selalu menjaga keamanan informasi pribadi mereka dan tidak memberikan informasi pribadi kepada pihak yang tidak dapat dipercaya [12].

Di Indonesia, pelaku typosquatting dapat dikenakan sanksi hukum berdasarkan beberapa peraturan yang berlaku, antara lain:

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Pasal 36 ayat (1) ITE menyebutkan bahwa setiap orang yang dengan sengaja dan tanpa hak menggunakan atau memanfaatkan domain yang tidak sah atau tidak sesuai dengan peraturan yang berlaku, diancam dengan pidana kurungan paling lama 4 tahun dan/atau denda paling banyak Rp1 miliar [13].

Undang-Undang Republik Indonesia Nomor 5 Tahun 1997 tentang Penanggulangan Kejahatan Dunia Maya. Pasal 3 ayat (1) UU No. 5 Tahun 1997 menyebutkan bahwa setiap orang yang dengan sengaja dan tanpa hak memasukkan, mengubah, menghilangkan, atau menyalahgunakan data elektronik

[11] Jubaedi dan Irawan, "Perancangan Program Acara TelEvisi Menggunakan Teknik Editing Kinetic Typography."
[12] White dan Cornu, "Visitors and Residents: A new typology for online engagement."
[13] Akbar, "Analisa Perbandingan Transaksi Dengan Menggunakan Uang Elektronik (E-Money) Dan Dengan Menggunakan Kartu Kredit (Studi Kasus Pada Bank Bumn) Periode 2010-2015."

atau sistem elektronik, diancam dengan pidana penjara paling lama 6 tahun dan/atau denda paling banyak Rp1 miliar.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 20 Tahun 2016 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pasal 34 ayat (1) Permenkominfo No. 20 Tahun 2016 menyebutkan bahwa setiap orang yang dengan sengaja dan tanpa hak menggunakan atau memanfaatkan domain yang tidak sah atau tidak sesuai dengan peraturan yang berlaku, diancam dengan pidana kurungan paling lama 4 tahun dan/atau denda paling banyak Rp1 miliar.

Selain sanksi hukum yang ditetapkan dalam peraturan di atas, pelaku typosquatting juga dapat dikenakan sanksi dari lembaga-lembaga yang bertanggung jawab terhadap keamanan internet, seperti Internet Corporation for Assigned Names and Numbers (ICANN) atau organisasi lainnya yang bertugas mengatur penggunaan domain di internet [14].

3.3 Solusi Korban Kejahatan Typosquatting

Jika Anda merasa menjadi korban kejahatan typosquatting, ada beberapa tindakan yang dapat Anda lakukan untuk mengatasinya, antara lain:

Segera hubungi lembaga penanganan kejahatan teknologi informasi. Di Indonesia, Anda dapat menghubungi Badan Siber dan Sandi Negara (BSSN) atau lembaga penanganan kejahatan teknologi informasi lainnya untuk meminta bantuan [15].

Laporkan kejahatan tersebut kepada lembaga terkait. Anda dapat melaporkan kejahatan typosquatting yang menimpa Anda kepada lembaga penanganan kejahatan teknologi informasi, seperti BSSN atau lembaga lainnya. Pastikan untuk menyertakan semua bukti yang Anda miliki dalam laporan tersebut.

Beritahu teman dan keluarga Anda. Agar tidak terjadi lagi kepada mereka, segera beritahu teman dan keluarga Anda jika Anda menjadi korban kejahatan typosquatting. Beritahu mereka tentang cara menghindari kejahatan tersebut dan meminta agar mereka juga tidak salah memasukkan

alamat URL saat ingin mengakses sebuah website.

Hapus malware yang terinfeksi. Jika Anda terinfeksi oleh malware melalui website palsu yang dibuat oleh pelaku typosquatting, segera hapus malware tersebut dari perangkat Anda. Anda dapat menggunakan antivirus atau antimalware untuk menghapus malware tersebut.

Ganti sandi yang terkompromisi. Jika informasi pribadi Anda tersebar dan sandi Anda terkompromisi, segera ganti sandi yang Anda gunakan untuk login ke akun-

[14] Dam, Klausner, dan Schrittwieser, "Typosquatting for Fun and Profit: Cross-Country Analysis of Pop-Up Scam."
[15] Betts dkk., "Adolescents' experiences of street harassment: creating a typology and assessing the emotional impact."

akun yang dimiliki. Gunakan sandi yang kuat dan tidak mudah ditebak oleh orang lain [16].

Hati-hati dengan tawaran yang tidak masuk akal. Jika Anda menerima tawaran yang tidak masuk akal atau tidak sesuai dengan yang diharapkan melalui email atau pesan lainnya, jangan mudah terkecoh dan memberikan informasi pribadi atau uang kepada pihak yang tidak dapat dipercaya [17].

Selalu waspada dan memastikan bahwa alamat URL yang dimasukkan sudah benar. Salah satu cara paling efektif untuk menghindari kejahatan typosquatting adalah dengan selalu memastikan bahwa alamat URL yang dimasukkan sudah benar sebelum mengakses sebuah website. Selain itu, Anda juga harus selalu menjaga keamanan informasi pribadi dan tidak memberikan informasi pribadi kepada pihak yang tidak dapat dipercaya. Selain itu, Anda juga dapat menggunakan alat bantu seperti antivirus atau antimalware untuk menghindari infeksi malware yang dapat menyebar melalui website palsu yang dibuat oleh pelaku typosquatting. Selalu memperhatikan keamanan informasi pribadi, seperti dengan menggunakan sandi yang kuat dan tidak menyimpan sandi di perangkat yang mudah diakses orang lain, juga merupakan cara yang efektif untuk menghindari kejahatan typosquatting.

4. **Simpulan**

Typosquatting adalah salah satu jenis kejahatan teknologi informasi yang dapat merugikan para pengguna internet. Pelaku typosquatting biasanya akan membuat website palsu yang mirip dengan website populer dengan menggunakan nama domain yang mirip, dengan tujuan untuk menyalahgunakan traffic yang salah sasaran atau bahkan melakukan phishing atau menyebarkan malware. Dampak yang ditimbulkan oleh typosquatting bisa sangat merugikan, seperti kehilangan informasi pribadi, uang, kerusakan pada perangkat, dan kerugian reputasi.

Untuk menghindari kejahatan typosquatting, para pengguna internet harus selalu waspada dan memastikan bahwa mereka tidak salah memasukkan alamat URL saat ingin mengakses sebuah website. Selain itu, pengguna juga harus selalu menjaga keamanan informasi pribadi dan tidak memberikan informasi pribadi kepada pihak yang tidak dapat dipercaya. Selain itu, menggunakan alat bantu seperti antivirus atau antimalware, serta memperhatikan keamanan informasi pribadi dengan menggunakan sandi yang kuat dan tidak menyimpan sandi di perangkat yang mudah diakses orang lain, juga dapat membantu menghindari kejahatan typosquatting.

[16] Clark, "The Truth in Domain Names Act of 2003 and a Preventative Measure to Combat Typosquatting."
[17] Lipton, "Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property, and Restitution."

Jika Anda menjadi korban kejahatan typosquatting, ada beberapa tindakan yang dapat Anda lakukan untuk mengatasinya, seperti menghubungi lembaga penanganan kejahatan teknologi informasi, melaporkan kejahatan tersebut kepada lembaga terkait, memberitahu teman dan keluarga Anda, menghapus malware yang terinfeksi, mengganti sandi yang terkompromisi, dan selalu waspada terhadap tawaran yang tidak masuk akal. Dengan demikian, Anda dapat meminimalisir risiko menjadi korban kejahatan typosquatting dan menjaga keamanan informasi pribadi Anda di internet.

Daftar Pustaka

Adebayo, Omotosho, Awazie Divine, Ayegba Peace, dan Emuoyibofarhe Justice. "A Gamified Technique to Improve Users' Phishing and Typosquatting Awareness." *Communications in computer and information science* 1350 (12 Agustus 2021): 403–14. https://lens.org/149-203-285-490-158.

Akbar, Akhmad. "Analisa Perbandingan Transaksi Dengan Menggunakan Uang Elektronik (E-Money) Dan Dengan Menggunakan Kartu Kredit (Studi Kasus Pada Bank Bumn) Periode 2010-2015," 2019. https://doi.org/10.33753/mandiri.v3i1.59.

Bakhareva, Olena. "Objects of intellectual property rights: general terms of protection." *Theory and Practice of Intellectual Property*, no. 6 (16 Juni 2021): 98–106. https://doi.org/10.33731/62020.233970.

Banerjee, Anirban, Sazzadur Rahman, dan Michalis Faloutsos. "SUT: Quantifying and mitigating URL typosquatting." *Computer Networks* 55, no. 13 (2011): 3001–14. https://doi.org/10.1016/j.comnet.2011.06.005.

Betts, Lucy R., Rachel Harding, Sheine Peart, Catarina Sjolin Knight, David L. Wright, dan Kendall Newbold. "Adolescents' experiences of street harassment: creating a typology and assessing the emotional impact." *Journal of Aggression, Conflict and Peace Research* 11, no. 1 (11 Februari 2019): 38–46. https://doi.org/10.1108/jacpr-12-2017-0336.

Clark, Christopher G. "The Truth in Domain Names Act of 2003 and a Preventative Measure to Combat Typosquatting." *Cornell Law Review* 89, no. 6 (2004): 1476-. https://lens.org/199-523-059-008-411.

Dam, Tobias, Lukas Daniel Klausner, dan Sebastian Schrittwieser. "Typosquatting for Fun and Profit: Cross-Country Analysis of Pop-Up Scam." *Journal of Cyber Security and Mobility* 9 (25 Maret 2020): 265-300-265–300. https://doi.org/10.13052/jcsm2245-1439.924.

Dewi, Adityas Widayani. "Kejahatan Teknologi Hacking Paypal," 10 November 2011. https://lens.org/075-138-349-725-956.

Jubaedi, Ahmad Dedi, dan Doddy Irawan. "Perancangan Program Acara TELEvisi Menggunakan Teknik Editing Kinetic Typography." *ProTekInfo(Pengembangan Riset dan Observasi Teknik Informatika)* 2 (19 Januari 2017): 12–19. https://doi.org/10.30656/protekinfo.v2i0.43.

Lipton, Jacqueline D. "Bad Faith in Cyberspace: Grounding Domain Name Theory in Trademark, Property, and Restitution." *Harvard Journal of Law & Technology* 23, no. 2 (11 Agustus 2009): 447-. https://lens.org/139-193-490-914-547.

Peytchev, Andy, dan Scott Crawford. "A Typology of Real-Time Validations in Web-Based Surveys." *Social Science Computer Review* 23, no. 2 (2005): 235–49. https://doi.org/10.1177/0894439304273272.

Rong, Gao. "Discuss of Typological of the Intellectual Property Crime." *Journal of Jiangxi Public Security College*, 2010. https://lens.org/048-686-710-517-09X.

White, David, dan Alison Le Cornu. "Visitors and Residents: A new typology for online engagement." *First Monday* 16, no. 9 (23 Agustus 2011). https://doi.org/10.5210/fm.v16i9.3171.