BAB I

PENDAHULUAN

A. Latar Belakang Masalah

Perkembangan pesat dari teknologi berubah seiring perkembangan zaman, terlebih khusus mengenai teknologi informasi yang berbasis pada komputer sebagai wadah penyimpanan informasi-informasi tersebut. Mengamati situasi terkini, terutama di Indonesia, keprihatinan mendalam muncul mengenai potensi dampak negatif yang dapat ditimbulkan oleh kemajuan teknologi terhadap kehidupan sosial masyarakat Indonesia. Terkait dengan hal ini, perlu adanya peningkatan kesadaran masyarakat terhadap lingkungan sekitarnya. Perubahan yang terjadi dengan cepat sebagai hasil dari kemajuan teknologi, baik secara sadar maupun tanpa disadari, telah mengubah pola hidup masyarakat Indonesia dalam beberapa aspek. Sebagai contoh, sekarang banyak anak yang mengalami ketergantungan pada perangkat gadget mereka dan bahkan pada orang tua mereka. Efek negatif lainnya adalah melambatnya perkembangan keterampilan sosialisasi di kalangan masyarakat akibat fokus yang berlebihan pada penggunaan gadget. Di Indonesia, peran media massa, teknologi, dan media sosial semakin dominan. Hal ini memiliki kemampuan yang signifikan untuk mempengaruhi opini publik dengan cepat dan mudah.[1]

---

[1] Fitriani Y, ”Pemanfaatan media sosial sebagai media penyajian konten edukasi atau pembelajaran digital”, *JISAMAR (Journal of Information System, Applied, Management, Accounting and Research),* Vol.5, No.4, (September 2021) hlm1006-1013.

Internet sebagai bagian pendukung dalam sebuah teknologi. Sehingga membuat internet menjadi faktor utama penunjang kelancaran penggunaan teknologi dalam jaringan saat ini. Sebagai sebuah jaringan dalam komputer yang mampu tersalurkan ke seluruh dunia, internet disebut sebagai jalur transportasi segala informasi yang berbentuk file atau data pada computer lain. Dengan kata lain, tanpa adanya jaringan internet segala bentuk informasi atau dokumen yang tersimpan dalam sebuah komputer tidak dapat digunakan demi penyebaran informasi ke dalam komputer yang lain.[2]

Manusia yang berada hampir di seluruh belahan dunia sangat bergantung dengan keberadaan internet bahkan dengan menggunakan jaringan internet, telah mampu membentuk budaya baru di dalam kehidupan. Internet merubah pekerjaan sehari-hari menjadi lebih mudah dalam berbagai sektor mulai dari kegiatan perdagangan, bisnis, pembayaran atau transaksi perbankan yang dapat dimanfaatkan untuk kepentingan pribadi, instansi/perusahaan atau pun pemerintahan. Semakin banyaknya aktifitas yang dimanfaatkan oleh internet ini, mengakibatkan peningkatan pengguna internet di seluruh dunia. Oleh karena itu, berkenaan dengan pembangunan, kemajuan dan perkembangan teknologi informasi melalui internet, peradaban manusia diperhadapkan pada fenomena-fenomena baru yang mampu mengubah hampir setiap aspek kehidupan manusia.[3]

Data pengguna internet merujuk pada informasi yang menggambarkan

---

[2] Y. Maryono, B Patmi Istiana, 2008, *Teknologi Informasi & Komunikasi 3*, Jakarta, Quadra, hlm.102

[3] Dikdik M, Elisatris Gultom, 2009, *Cyber Law Aspek Hukum dan Teknologi InformasI*, Bandung, PT. Refika Aditama, hlm.90

jumlah individu atau pengguna yang menggunakan layanan internet. Data ini mencakup informasi seperti jumlah pengguna internet, tingkat penetrasi internet di suatu wilayah atau negara, serta karakteristik demografis dari pengguna internet tersebut. Terdapat Data pengguna Internet baik pengguna Global maupun Nasional. Menurut laporan "Digital 2021: Global Overview Report" yang diterbitkan oleh Data Reportal, pada Januari 2021 terdapat sekitar 4,66 miliar pengguna internet di seluruh dunia. Pengguna internet paling banyak berasal dari wilayah Asia, dengan sekitar 2,82 miliar pengguna. Negara dengan jumlah pengguna internet terbesar adalah Tiongkok, dengan lebih dari 900 juta pengguna.[4] Menurut hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), jumlah pengguna internet di Indonesia pada tahun 2022-2023 mencapai 215,63 juta orang. Peningkatan ini sebesar 2,67% dibandingkan dengan periode sebelumnya yang sebanyak 210,03 juta pengguna. Sementara itu, menurut We Are Social dan Meltwater, jumlah pengguna internet di Indonesia per Januari 2023 tercatat mencapai 212,9 juta orang. Jumlah ini naik dari tahun sebelumnya, di mana pada 2022 lalu, We Are Social menyebut jumlah pengguna internet di Indonesia berkisar 202 juta. Jumlah pengguna internet di Indonesia ini setara dengan 77% dari total populasi Indonesia yang sebanyak 276,4 juta orang pada awal tahun 2023.[5]

[4] Data Reportal Digital: Global Overview Report, 2021, (*DIGITAL 2021: GLOBAL OVERVIEW REPORT)*, https://datareportal.com/reports/digital-2021-global-overview-report, (diakses pada 27 Januari 2021 pukul 19.30)

[5] APJI, 2023,*(Survei Internet APJI)*, Asosiasi Penyelenggara Jasa Internet Indonesia (apjii.or.id), (diakses pada 15 Mei 2023 pukul 15.00 - 18.00)

Perkembangan pesat dalam teknologi dan akses yang lebih mudah ke internet telah memicu peningkatan pesat dalam aktivitas transaksi elektronik. Di Era di mana berbagai aspek kehidupan, termasuk bisnis, keuangan, komunikasi, dan hiburan, semuanya berpusat pada transaksi dan interaksi elektronik. Namun, dengan peningkatan ini, juga muncul tantangan baru yang signifikan dalam bentuk tindak kejahatan *Phishing. Kejahatan* adalah ancaman yang tak bisa diabaikan dalam dunia maya. Pelaku mencari dan mengeksploitasi kelemahan sistem serta tingkat kesadaran yang bervariasi dari para pengguna terhadap keamanan sistem informasi. Pelaku menggunakan teknik canggih dan seringkali tidak terdeteksi untuk meretas sistem, mencuri informasi sensitif, melakukan penipuan, dan bahkan menyebarkan malware yang dapat menyebabkan kerugian besar.[6]

Teknologi internet memfasilitasi akses informasi dan interaksi antarindividu secara cepat dan global. Namun, dengan ketergantungan yang semakin besar pada teknologi ini, resiko *Phishing* juga meningkat. Faktanya, kegiatan transaksi elektronik dapat diibaratkan sebagai pedang bermata dua. Hal ini disebabkan oleh dampak positif yang dihasilkan dari penggunaan transaksi elektronik, seiring dengan munculnya dampak negatif yang juga turut menyertainya. Penting untuk diakui bahwa transaksi elektronik, meskipun memberikan manfaat bagi penggunanya, juga membuka peluang bagi tindakan melawan hukum.[7]

---

[6] Muhamad Yusuf Tri Setio, 2020, *Sistem Manajemen Risiko pada Transaksi Online di Merchant e-commerce,* Jakarta, PPM Manajemen, hlm.21

[7] Smith, A, "The Dual Nature of Electronic Transactions: Positive Advancements and Cybercrime Risks", *Journal of Cybersecurity and Digital Ethics,* Vol.5, No.3, (Januari, 2018), hlm 230

Beberapa dampak positif transaksi elektronik adalah kemudahan dan keterjangkauan, memungkinkan kita untuk melakukan pembelian dan pembayaran secara online dengan mudah dan cepat, serta berbelanja kapan saja dan di mana saja tanpa harus pergi ke toko fisik. Selain itu, transaksi elektronik juga memberikan akses ke produk dan layanan yang mungkin sulit dijangkau di wilayah tertentu. Efisiensi juga menjadi salah satu dampak positif, dengan transaksi elektronik yang mempercepat proses pembayaran dan pengiriman barang, menghemat waktu dan tenaga tanpa perlu antri di kasir atau mengisi formulir secara manual. Keamanan juga menjadi fokus, di mana transaksi elektronik menggunakan protokol keamanan canggih seperti enkripsi data dan otentikasi dua faktor untuk melindungi informasi pribadi dan keuangan, membantu mencegah penipuan dan akses yang tidak sah.[8]

Transaksi elektronik, meskipun membawa dampak positif, juga memiliki sejumlah dampak negatif yang perlu diperhatikan. Salah satu risiko utama adalah terkait dengan keamanan dan privasi, di mana transaksi yang tidak dilindungi dengan baik dapat mengakibatkan pencurian identitas dan penipuan online, yang berpotensi mengekspos data pribadi dan finansial. Selain itu, ketergantungan pada teknologi yang semakin meningkat dapat menyebabkan ketidaknyamanan dan kerugian finansial bagi konsumen jika terjadi gangguan jaringan atau kerusakan sistem. Ketimpangan akses terhadap transaksi elektronik juga merupakan dampak negatif yang patut diperhatikan.

[8] Gunawan Widjaja & Ahmad Yani, 2001, *Hukum Tentang Perlindungan Konsumen*. Jakarta, PT Gramedia Pustaka Utama, hlm.57

Masih ada sebagian masyarakat yang tidak memiliki akses atau pemahaman yang cukup terhadap teknologi, menciptakan ketidaksetaraan akses terhadap transaksi elektronik di berbagai wilayah. Risiko keuangan juga menjadi aspek penting yang berkaitan dengan transaksi elektronik, terutama dalam hal penyalahgunaan kartu kredit dan potensi kehilangan dana elektronik. Keberhatian dalam melindungi informasi keuangan menjadi krusial untuk menghindari risiko finansial yang mungkin timbul. Selain itu, perkembangan transaksi elektronik juga dapat berdampak pada sektor pekerjaan tradisional, mengakibatkan pengangguran karena adopsi teknologi dapat mengurangi jumlah pekerjaan di toko fisik dan sektor perdagangan tradisional. Penting untuk memahami dan mengelola risiko-risiko yang terkait untuk memastikan penggunaan teknologi yang lebih aman dan berkelanjutan.[9]

Kegiatan *Phishing* umumnya mengincar industri-industri yang beroperasi secara daring, termasuk sektor perdagangan barang maupun jasa. Dalam mencoba menyamar, para pelaku kejahatan akan mengganti identitas mereka agar terlihat seolah-olah berasal dari pihak yang sah, misalnya melalui teman atau keluarga dengan cara mengirimkan sebuah aplikasi melalui Sosial Media. Seringkali, para pihak yang di rugikan diarahkan ke situs web palsu melalui tautan yang bertujuan untuk meminta pihak yang di rugikan untuk membagikan data pribadi mereka. Upaya ini dimaksudkan untuk melakukan penipuan terhadap pihak yang di rugikan dan mendapatkan akses ilegal ke

[9] Syarifuddin, 2023, *Perkembangan Teknologi "Ancaman Atau Peluang" Perkembangan Teknologi "Ancaman Atau Peluang"*, https://sulselprov.go.id/post/perkembangan-teknologi-ancaman-atau-peluang (diakses pada 5 Juli 2023 pukul 13.30)

informasi sensitif yang dapat digunakan untuk kegiatan ilegal lebih lanjut.[10]

Kejadian *Phishing* semakin meningkat, Menurut laporan CNBC Indonesia, mencatat bahwa jumlah kasus peretasan di Indonesia selama tahun 2020 cukup signifikan. Seiring dengan meningkatnya jumlah pengguna internet selama pandemi Covid-19, peretasan yang banyak dilakukan melalui email *Phishing* mencapai puncaknya pada kuartal II tahun lalu, terutama antara bulan Maret hingga Mei 2020. Peningkatan signifikan dalam kasus email *Phishing* terutama terjadi selama jam kerja.[11] Dalam kuartal pertama tahun 2023, kasus serangan *Phishing* paling banyak terjadi pada bulan Februari dengan jumlah aduan mencapai 15.050 kasus. Sementara itu, jumlah aduan pada bulan Januari sekitar 7.665 kasus, dan di bulan Maret sebanyak 3.960 kasus. Dari data ini dapat disimpulkan bahwa kejahatan *Phishing* sangat marak terjadi di seluruh dunia.[12]

Laporan dari Surf Shark mencatat sekitar 820 ribu kasus pembobolan di Indonesia selama kuartal kedua tahun 2022. Tingginya kasus kebocoran data di internet membuat Indonesia menduduki peringkat pertama sebagai negara dengan tingkat pembobolan data tertinggi di kawasan ASEAN (*Association of Southeast Asian Nations*). Kebocoran data di Indonesia pada kuartal kedua tahun 2022 mengalami peningkatan sebesar 143%

---

[10] Yustitiana, R., ”Pelaksanaan Pengaturan Hukum Tindak Kejahatan Fraud Phising Transaksi Elektronik Sebagai Bagian dari Upaya Penegakan Hukum di Indonesia Dikaitkan dengan Teori Efektivitas Hukum” *Jurnal Hukum Visio Justisia*, Vol.1 No.1, (Juni, 2021), hlm.105.

[11] Anisatul Umah, 2021, *Serangan Phishing Indonesia Makin Merajalela*, https://www.cnbcindonesia.com/tech/20210306162132-37-228322/kasus-phishing-email-yang-serang-indonesia-makin-merajalela# (diakses pada 6 Maret 2021, pukul 18.03)

[12] Muhamad Firstian P.A, 2023, *Meningkatnya Serangan Phishing di Indonesia: Data Terbaru yang Mengejutkan*, https://blog.wowrack.co.id/2023/09/21/meningkatnya-serangan-phishing-di-indonesia-data-terbaru-yang-mengejutkan/ (diakses pada 21 September pukul 09.00)

dibandingkan dengan kuartal pertama tahun 2022. Menurut Surf Shark, sejak tahun 2004, total kasus kebocoran data di Indonesia mencapai 120,9 juta laporan. Jumlah akun yang mengalami kebocoran data pada kuartal kedua tahun 2022 mengalami peningkatan 2% secara global, mencapai 459 akun yang dibobol setiap menit, dibandingkan dengan kuartal sebelumnya yang mencapai 450 akun per menit.[13]

Pada tahun 2001, Indonesia dihebohkan oleh sebuah insiden serupa dengan unsur *Phishing.* Kejadian ini terjadi ketika layanan *internet banking*, sebagai sarana pemanfaatan transmisi elektronik di sektor perbankan, baru dimulai oleh bank-bank di Indonesia. Peristiwa tersebut menimpa Bank Central Asia (BCA), di mana pelaku membeli 6 domain palsu dengan nama yang mirip dengan situs resmi *www.klikbca.com.* Akibatnya, nasabah BCA salah mengidentifikasi salah satu situs palsu tersebut sebagai situs resmi dari *internet banking* BCA, sehingga user id dan PIN yang dimasukkan oleh nasabah saat login tercatat di situs palsu tersebut dan tersimpan dalam *Hard Disk* komputer pelaku pada saat itu.[14]

Keberadaan praktik *Phishing* di Indonesia telah menjadikan transaksi elektronik sangat rentan dan menimbulkan keprihatinan. Hal ini diperparah dengan sebaran pengguna internet yang meliputi berbagai kalangan masyarakat di Indonesia. Kerugian dari serangan *Phishing* melibatkan pencurian identitas, kehilangan keuangan signifikan, kerusakan reputasi bagi

---

[13] *Ibid*

[14] Malunsenge, Leticia, Cornelis Massie, and Ronald Rorie. "Penegakan Hukum Terhadap Pelaku Dan Korban Tindak Pidana Cyber Crime Berbentuk Phising Di Indonesia", *Journal Lex Crimen*, Vol.11 No.3, (April, 2022), hlm.202.

bisnis atau organisasi, ketidaknyamanan dan gangguan bagi pihak yang di rugikan, potensi kejahatan lainnya yang melibatkan dampak psikologis, dan penyebaran informasi palsu. Oleh karena itu, diperlukan perlindungan hukum yang efektif untuk melindungi pihak yang di rugikan *Phishing.* Penting juga untuk meningkatkan kesadaran masyarakat terkait taktik dan risiko *Phishing* guna memitigasi dampak yang ditimbulkan dan melindungi keamanan data pribadi mereka.[15]

Indonesia telah merumuskan sejumlah peraturan perundang-undangan terkait dengan transaksi elektronik, di antaranya Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain itu, terdapat berbagai regulasi lain yang terkait dengan transaksi elektronik di Indonesia. Namun, meskipun regulasi ini telah ada, fenomena kejahatan transaksi elektronik, khususnya yang terkait dengan *Phishing* yang terus mengemuka seiring dengan perkembangan teknologi dan semakin meluasnya transaksi online.[16]

Tujuan utama dari pengaturan perundang-undangan adalah untuk memberikan kepastian hukum terhadap suatu kegiatan dengan menguraikan apa yang diizinkan dan tidak diizinkan dalam pelaksanaannya. Selain itu, tujuan lainnya adalah untuk mencegah kemungkinan risiko di masa mendatang yang dapat merugikan pihak-pihak yang terlibat sebagai warga negara. Terlepas dari hal tersebut, patut diakui bahwa fenomena yang tengah

---

[15] N.P. Singh, "Online Frauds in Banks with Phishing," *Journal of Internet Banking and Commerce*, Vol 12, No. 2 (Agustus, 2007), hlm 4

[16] *Kitab Undang-Undang Hukum Pidana Republik Indonesia.* (Kitab Undang-Undang Hukum Pidana, KUHP).

terjadi di Indonesia, khususnya dalam konteks meningkatnya transaksi elektronik, turut diikuti dengan peningkatan kejahatan transaksi elektronik, seperti upaya penipuan melalui *Phishing*.[17]

Secara rinci, pasal dalam Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menjelaskan perbuatan yang dianggap melanggar hukum terkait dengan penipuan situs *Phishing*. Undang-Undang ini memandang penipuan situs sebagai tindakan kriminal yang mengambil keuntungan dari perkembangan sistem teknologi.[18] Dalam menghadapi tantangan *Phishing*, terdapat kebutuhan mendesak untuk melindungi pengguna internet di era digital yang terus berkembang. Meskipun demikian, sistem hukum yang ada saat ini memiliki kelemahan, khususnya dalam lingkup Undang-Undang Informasi dan Transaksi Elektronik. Undang Undang ini belum sepenuhnya dapat meningkatkan perlindungan terhadap pihak yang di rugikan.[19] *Phishing* dapat dikenakan Pasal 28 Ayat (1) jo Pasal 45A Ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik karena terbukti melakukan manipulasi dan tindakan kebohongan yang merugikan pihak lain.[20]

---

[17] Ronny Hanitijo Soemitro, 1990, *Metode Penelitian Hukum dan Jurimetri*, Jakarta, Ghalia Indonesia, hlm 59-65.

[18] Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[19] Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[20] Ardi Saputra Ardi Saputra Gulo, ”*Cyber Crime dalam bentuk Phishing Berdasarkan Undang-Undang Informasi dan Transaksi Elektronik”, 1 PAMPAS, Journal Of Criminal,* Vol.1.2, (2020), h. 68-81.)

Penanganan *Phishing* menjadi suatu prioritas yang sangat penting untuk memastikan perlindungan masyarakat dari dampak negatif yang dihasilkan oleh tindakan kejahatan ini. Pemerintah dan otoritas terkait harus memprioritaskan tindakan yang efektif dalam menanggapi masalah ini dan menyediakan perlindungan yang memadai bagi masyarakat. Dalam konteks ini, diperlukan penelitian mendalam dan analisis yang komprehensif untuk memahami lebih baik dan merumuskan strategi penanggulangan kejahatan *Phishing*, agar dapat ditemukan solusi dan upaya yang efektif untuk mengatasi masalah ini.[21]

Penelitian ini tidak hanya memberikan wawasan yang mendalam tentang perlindungan hukum yang diatur oleh Undang-Undang Nomor 19 Tahun 2016, tetapi juga mengidentifikasi potensi ketidaksesuaian dan tantangan spesifik yang dihadapi di lingkungan transaksi elektronik Kota Yogyakarta. Penelitian ini terletak pada pemahaman mendalam terhadap kerangka hukum yang mengatur transaksi elektronik di tingkat lokal, mengingat setiap daerah dapat memiliki dinamika dan karakteristik tersendiri. Identifikasi tantangan dan risiko yang spesifik di Kota Yogyakarta dapat memberikan dasar bagi pihak berwenang untuk merancang dan mengimplementasikan kebijakan perlindungan yang lebih cermat dan relevan. Dengan memahami implementasi undang-undang ini secara kontekstual, penelitian ini juga memiliki potensi untuk memberikan

[21] Wibisono A, "*Cybercrime Laws and Their Effectiveness: A Comparative Study", Journal of Cybersecurity Policy and Law*, Vol. 11 No (1), (2020) hlm 39-54.

rekomendasi yang dapat meningkatkan efektivitas dan responsibilitas dalam melindungi masyarakat Yogyakarta dari potensi serangan *Phishing* dan memberikan kontribusi dalam meningkatkan tingkat kesadaran hukum di kalangan masyarakat, yang menjadi kunci untuk melibatkan mereka secara aktif dalam melindungi diri mereka sendiri dan mendukung upaya pencegahan.

Berdasarkan latar belakang yang sudah di uraikan diatas maka penulis mengambil judul "Perlindungan Hukum Terhadap Tindakan *Phishing* Dalam Transaksi Elektronik Berdasarkan Undang-Undang Nomor 19 Tahun 2016 Di Kota Yogyakarta". Tujuan dari penelitian ini adalah untuk menganalisis dan memahami perlindungan hukum yang diberikan oleh Undang-Undang Nomor 19 Tahun 2016 terhadap tindakan *Phishing* dalam transaksi elektronik, dengan fokus pada implementasi dan dampaknya di wilayah Kota Yogyakarta.

B. Perumusan Masalah

1. Bagaimana pencegahan *Phishing* yang dapat di lakukan penegak hukum di Kota Yogyakarta?
2. Bagaimana upaya ganti rugi terhadap pihak yang di rugikan yang terkena *Phishing* di Kota Yogyakarta?

C. Tujuan Penelitian

Tujuan penelitian dari rumusan masalah di atas adalah sebagai berikut:

1. Untuk mengidentifikasi dan menganalisis upaya pencegahan tindakan *Phishing* yang diatur oleh Undang-Undang di Kota Yogyakarta, dengan

fokus pada implementasi Undang-Undang Nomor 19 Tahun 2016.

2. Untuk mengevaluasi efektivitas mekanisme upaya ganti rugi yang tersedia bagi pihak yang di rugikan *Phishing* di Kota Yogyakarta sesuai dengan ketentuan yang terdapat dalam Undang-Undang Nomor 19 Tahun 2016.

D. Manfaat Penelitian

Penelitian dengan judul "**PERLINDUNGAN HUKUM TERHADAP TINDAKAN *PHISHING* DALAM TRANSAKSI ELEKTRONIK BERDASARKAN UNDANG-UNDANG NOMOR 19 TAHUN 2016 DI KOTA YOGYAKARTA**" memiliki beberapa manfaat yang signifikan:

1. Manfaat Teoritis
    a. Memberikan pemahaman yang lebih mendalam tentang fenomena *Phishing* dan bagaimana hal tersebut dapat dicegah melalui Undang-Undang di Kota Yogyakarta.
    b. Mempertajam pemahaman mengenai hubungan antara Undang-Undang Nomor 19 Tahun 2016 dan upaya ganti rugi terhadap pihak yang di rugikan *Phishing* di Kota Yogyakarta.
    c. Menghasilkan pemahaman yang lebih luas tentang relevansi dan efektivitas Undang-Undang dalam mencegah dan menangani kasus *Phishing* di Indonesia secara umum.
2. Manfaat Praktis
    a. Memberikan rekomendasi dan panduan kepada pihak yang berwenang atau instansi terkait di Kota Yogyakarta untuk meningkatkan

pencegahan *Phishing* berdasarkan peraturan yang telah ada, guna melindungi masyarakat dari ancaman tersebut.

b. Memberikan panduan kepada pihak yang di rugikan *Phishing* di Kota Yogyakarta dalam memperoleh upaya ganti rugi yang sesuai dengan ketentuan yang terdapat dalam Undang-Undang Nomor 19 Tahun 2016.

c. Menyediakan informasi yang berguna untuk masyarakat umum mengenai hak dan upaya hukum terhadap kasus *Phishing*, sehingga dapat meningkatkan kesadaran dan pengetahuan mereka dalam melindungi diri dari serangan *Phishing*.