

---

## Setan Scammer : Menghindari Penipuan Online

**Martha Surya Dinata Mendrofa<sup>1</sup>, Asnita Julianti Waruwu<sup>2</sup>, Celine Ivana Radjagukguk<sup>3</sup>, Juang Saputra Zai<sup>4</sup>, Arivin Ilham<sup>5</sup>, Silfanny Ramadani Marunduri<sup>6</sup>, Nadia Seprina Cui<sup>7</sup>, Antonia Lisna Bate'e<sup>8</sup>, Bobi Setiawan Hulu<sup>9</sup>, Artika Memori Laoli<sup>10</sup>, Majesti Mendrofa<sup>11</sup>, Lusiana Ingat Sri Juni Zebua<sup>12</sup>**

<sup>123456789101112</sup> Fakultas Ekonomi Universitas Nias, Gunungsitoli, Indonesia

martha.mendrofa@gmail.com<sup>1</sup>, nitalian77@gmail.com<sup>2</sup>, celineivana23@gmail.com<sup>3</sup>, juangzai2020@gmail.com<sup>4</sup>, ariviniham907@gmail.com<sup>5</sup>, silvanyramadhani@gmail.com<sup>6</sup>, nadiaseprinac@gmail.com<sup>7</sup>, lisnabatele@gmail.com<sup>8</sup>, setiawanulu3@gmail.com<sup>9</sup>, artikamemorilaoliartika@gmail.com<sup>10</sup>, majesti242@gmail.com<sup>11</sup>, junizebuuaa@gmail.com<sup>12</sup>

### *Abstract*

The main purpose of implementing the seminar with the theme (satan scammer: online fraud) is to provide education to the people of Olora village to be more aware of various modes of digital fraud. The methods used are Community Education, training, mediation, science and technology simulation, science and technology substitution. The results of the PKM explain that Fraud Mode 1: Taking Advantage of Emotions & Urgency, Fraud Mode II: False Opportunities, Prevention Strategies that can be done include Identity verification: When there is a message asking for confirmation of the request. Make sure that the message is from an official source. This can be seen from the check mark symbol in the upper right corner of the sender and use a strong and unique password: Use a strong password that is not easily guessed by anyone. The conclusion in dealing with the many online frauds today, we as young people must be more active in finding out tricks so as not to get caught in this online fraud, so that by knowing we can anticipate and fortify our parents so that they are not tempted by all forms of online fraud.

**Keywords:** Scammer, Online Fraud

### **Abstrak**

Tujuan utama pelaksanaan seminar dengan tema (setan scammer : penipuan online) adalah untuk memberikan edukasi kepada masyarakat desa olora agar semakin waspada terhadap berbagai modus penipuan digital ini. Metode yang digunakan adalah Pendidikan Masyarakat, pelatihan, mediasi, simulasi Ipkteks, substitusi Ipkteks. Hasil PKM menjelaskan bahwa Modus Penipuan 1 : Memanfaatkan Emosional & Urgensi, Modus Penipuan II: Peluang Palsu, Strategi Pencegahan yang dapat dilakukan antara lain verifikasi Identitas : Ketika ada pesan yang meminta konfirmasi permintaan. Pastikanlah bahwa itu pesan dari sumber yang sudah resmi. Hal ini nampak pada simbol centang yang ada disudut kanan atas si pengirim serta gunakan kata sandi yang kuat dan Unik : Gunakan kata sandi yang kuat dan tidak mudah ditebak oleh siapapun. Kesimpulan dalam menghadapi banyaknya penipuan online saat ini, kita sebagai kaum muda harus lebih aktif dalam mencari tau trik agar tidak terjebak dalam penipuan online ini, sehingga dengan kita tahu maka kita bisa mengantisipasi dan membentengi orang tua kita agar tidak tergiur dengan segala bentuk penipuan online.

**Kata Kunci :** Scammer, Penipuan Online

## **PENDAHULUAN**

### **Latar Belakang Masalah**

Scammer online adalah pelaku penipuan yang beroperasi melalui internet, dengan tujuan memperoleh keuntungan finansial atau informasi pribadi dari korban. Mereka

menggunakan berbagai modus operandi, seperti berpura-pura menjadi pihak terpercaya, menawarkan hadiah palsu, atau membuat janji-janji manis yang tidak masuk akal. Penipuan online di Indonesia sangat relevan untuk diangkat dalam jurnal ilmiah, mengingat penipuan online (scam) merupakan salah satu kejahatan yang terus meningkat seiring dengan pesatnya penggunaan teknologi informasi dan komunikasi di masyarakat.

Scammer adalah pelaku kejahatan penipuan yang beroperasi di dunia maya, atau secara umum, seseorang yang melakukan penipuan untuk mendapatkan keuntungan finansial atau informasi pribadi dari korban. Mereka memanfaatkan berbagai modus operandi, termasuk penipuan online, phishing, dan penawaran palsu, untuk mengeksploitasi kepercayaan dan ketidakpahaman korban (Juditha, 2015).

Kejahatan yang terjadi di kalangan masyarakat melalui media online sering kita sebut dengan cybercrime. Cybercrime dapat diartikan sebagai kegiatan ilegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global. Setiap orang mempunyai kebebasan untuk berkomunikasi, menikmati hiburan, dan mengakses apa saja yang menurutnya bisa mendatangkan keuntungan dan kesenangan melalui internet. Dengan adanya jaringan komputer seperti internet dan ruang lingkup internet yang semakin luas membuat masalah kriminalitas menjadi kompleks di lingkungan masyarakat.

Sebagai fenomena sosial yang terjadi di muka bumi ini, permasalahan tindak pidana mungkin tidak akan berakhir sejalan dengan dinamika sosial dan perkembangan yang terjadi di kalangan masyarakat. Seiring berjalannya waktu permasalahan tindak pidana ini nampaknya akan semakin terus berkembang dan tidak akan pernah surut baik dilihat dari segi kualitas maupun kuantitasnya. Perkembangan permasalahan tindak pidana ini sangat membuat keresahan bagi masyarakat dan pemerintah.

Adapun 5 modus penipuan online yang umumnya mengintai adalah phishing, pharming, sniffing, money mule, dan social engineering. Modus penipuan online yang satu ini merupakan bentuk yang paling sering ditemukan. Biasanya, phishing dilakukan melalui email atau pesan teks. Jenis penipuan di mana scammer mencoba untuk menipu agar mengungkapkan informasi pribadi disebut. Phishing adalah praktik penipuan di mana penyerang menyamar sebagai entitas atau orang yang memiliki reputasi baik untuk mengelabui pengguna agar mengungkapkan informasi sensitif (Maharani et al., 2024).

Phishing adalah jenis serangan siber yang melibatkan korban melalui email, panggilan telepon, atau pesan teks palsu. Serangan ini umumnya dilakukan oleh penyerang

yang menyamar sebagai orang lain, dengan harapan dapat memengaruhi target agar memberikan data sensitif seperti detail pembayaran dan kata sandi.

Phishing vs. smishing vs. vishing menggunakan rekayasa sosial, tetapi berbeda dalam cara penyerang menghubungi Anda. Phishing menggunakan email dengan halaman login palsu, smishing menggunakan pesan teks palsu, dan vishing menggunakan panggilan suara untuk mengekstrak informasi pribadi. Pesan smishing sering kali berisi tautan yang mengarahkan pengguna ke situs web yang mungkin tampak sah, tetapi sebenarnya mencuri nama pengguna, kata sandi, dan data lainnya saat pengguna masuk. Beberapa pesan bahkan dapat diam-diam memasang malware di perangkat seluler korban.

Setelah melakukan pengenalan, biasanya scammer akan menginfokan bahwa mereka menemukan masalah pada akun korban, atau sebaliknya, mereka menawarkan korban sebuah hadiah yang harus segera diklaim oleh korban. Cara ini dilakukan untuk mendapat data pribadi ataupun memperoleh sejumlah uang dari korban. Mereka melakukannya dengan berbagai metode termasuk rekayasa sosial, email (phishing) dan pesan teks (smishing), yang sering kali menyamar sebagai perusahaan, lembaga pemerintah, atau bahkan orang sungguhan dalam hidup Anda yang sah guna menciptakan rasa percaya palsu (Tertibi et al., 2023).

Penipu, ketika mereka tahu Anda sudah tahu, biasanya akan tetap berusaha meyakinkan Anda bahwa mereka nyata dan tidak berbahaya bagi Anda. Jika upaya mereka gagal, mereka akan beralih ke calon korban berikutnya. Mereka biasanya menargetkan banyak orang untuk meningkatkan peluang keberhasilan. Uang yang sudah ditransfer ke penipu kemungkinan besar sulit untuk kembali sepenuhnya, namun ada upaya yang bisa dilakukan untuk meminimalisir kerugian. Langkah pertama adalah segera melaporkan kejadian ini ke bank dan pihak kepolisian, serta mengumpulkan bukti-bukti seperti bukti transfer, percakapan dengan pelaku, dan nomor rekening pelaku.

Ada banyak modus penipuan lain yang dilakukan melalui WhatsApp (WA). Penipu sering menggunakan berbagai cara untuk menipu korban, mulai dari berpura-pura menjadi teman atau keluarga yang membutuhkan bantuan, hingga mengirimkan file APK yang berisi malware, atau tautan phishing.

Beberapa modus penipuan yang umum terjadi melalui WhatsApp:

#### 1. Modus Undangan Pernikahan Digital:

Penipu mengirimkan file APK undangan pernikahan palsu, yang sebenarnya adalah aplikasi berbahaya yang dapat mencuri data pribadi dan informasi keuangan.

2. Modus Penipuan Kurir:

Penipu menyamar sebagai kurir pengiriman paket dan meminta korban membayar biaya pengiriman yang tidak jelas atau mengarahkan korban untuk mengunduh file APK.

3. Modus Penipuan Tagihan:

Penipu mengirimkan tagihan palsu, seperti tagihan listrik (PLN) atau tagihan lainnya, dan meminta korban untuk melakukan pembayaran ke rekening tertentu.

4. Modus Penipuan Resi:

Penipu mengirimkan file APK yang berpura-pura menjadi resi pengiriman paket dan meminta korban untuk mengunduh dan membuka file tersebut.

5. Modus Penipuan OTP:

Penipu berusaha mendapatkan kode OTP (One-Time Password) korban, yang digunakan untuk mengakses akun WhatsApp korban atau akun perbankan.

6. Modus Phishing:

Penipu mengirimkan tautan palsu yang mengarahkan korban ke website palsu yang dirancang untuk mencuri data pribadi, seperti informasi kartu kredit, nomor rekening, atau data login.

7. Modus Pura-pura menjadi Teman atau Keluarga:

Penipu menghubungi korban melalui WhatsApp dan berpura-pura menjadi teman atau anggota keluarga yang sedang dalam situasi darurat dan membutuhkan uang.

Modus kejahatan ini memanfaatkan kecanggihan teknologi untuk menipu korban, baik dengan mengambil uang maupun data pribadi, dan sering kali sulit dideteksi karena pelaku menggunakan berbagai teknik yang semakin beragam dan canggih. Penipuan ini dapat terjadi dalam berbagai bentuk dan modus, yang sering kali memanfaatkan ketidakpahaman atau kepercayaan korban (Wahyuddin et al., 2024).

Ada beberapa korban penipuan online ini, salah satunya yaitu warga desa olora.

1. Seorang bapak berinisial M (47) menjadi korban penipuan melalui pesan whatApp dengan kerugian mencapai jutaan.
2. Seorang anak muda yang menjadi korban berinisial APZ (27) penipuan tentang investasi bodong melalui link, WhatApp, aplikasi (FF19) dengan kerugian mencapai jutaan rupiah.

Tujuan Pelaksanaan Seminar :

Tujuan utama pelaksanaan seminar dengan tema (setan scammer : penipuan online) adalah untuk memberikan edukasi kepada masyarakat desa olora agar semakin waspada terhadap

berbagai modus penipuan digital ini. Melalui edukasi ini, diharapkan masyarakat desa olara dapat :

- 1) Mengenali berbagai modus penipuan online ini seperti tawaran uang tunai, investasi bodong dll.
- 2) Memahami langkah-langkah pencegahan agar tidak menjadi korban selanjutnya seperti tidak sembarangan mengangkat nomor tidak dikenal, tidak sembarangan mengklik tautan, serta menjaga kerahasiaan data pribadi.
- 3) Meningkatkan kesadaran untuk segera melapor jika menjadi korban atau menemukan aktivitas mencurigakan, sehingga warga desa olara menjadi lebih aman.

Dengan demikian, edukasi ini menjadi kunci utama dalam menekan angka korban penipuan online dan membangun masyarakat yang lebih cerdas dan tanggap terhadap kejahatan digital.

## **TINJAUAN PUSTAKA**

### **Pengertian Scammer**

Scammer adalah pelaku kejahatan yang melakukan penipuan, baik secara online maupun offline, untuk mendapatkan keuntungan finansial atau informasi pribadi dari korbannya. Mereka memanfaatkan berbagai taktik manipulasi dan rekayasa sosial untuk meyakinkan korban agar menyerahkan uang, data, atau akses ke akun penting.

Scammer adalah pelaku penipuan yang menggunakan tipu muslihat, rangkaian kebohongan, nama palsu, atau keadaan palsu untuk menguntungkan diri sendiri atau orang lain secara melawan hukum.

#### **Ciri-Ciri Scammer:**

##### **1. Modus Penipuan:**

Scammer sering menggunakan berbagai modus, seperti penipuan investasi, penipuan hadiah, penipuan pekerjaan, atau berpura-pura menjadi pihak resmi (misalnya, bank, perusahaan, atau agen pemerintah).

##### **2. Taktik Manipulasi:**

Mereka sering menggunakan tekanan waktu, janji imbalan tinggi, atau ancaman untuk memanipulasi korban.

##### **3. Kurangnya Informasi Detail:**

Scammer cenderung menghindari memberikan informasi detail tentang diri mereka atau bisnis mereka.

#### 4. Desakan untuk Bertindak Cepat:

Mereka akan mendorong korban untuk segera mengambil tindakan tanpa berpikir panjang.

#### Cara Menghindari Scammer:

##### 1. Waspada terhadap Penawaran yang Terlalu Bagus:

Jika tawaran terdengar terlalu bagus untuk menjadi kenyataan, kemungkinan besar itu adalah penipuan.

##### 2. Verifikasi Informasi:

Jangan percaya begitu saja klaim atau informasi yang diberikan oleh orang yang tidak dikenal. Verifikasi informasi tersebut melalui sumber yang terpercaya.

##### 3. Lindungi Informasi Pribadi:

Jangan pernah memberikan informasi pribadi, seperti nomor rekening, PIN, atau data pribadi lainnya kepada pihak yang tidak dikenal.

##### 4. Laporkan Penipuan:

Jika Anda menjadi korban penipuan, segera laporkan ke pihak berwajib.

Dengan memahami pengertian, ciri-ciri, dan modus operandi scammer, serta cara menghindarinya, Anda dapat lebih aman dan terlindungi dari kejahatan penipuan, terutama di dunia digital yang semakin kompleks.

## **METODE PELAKSANAAN**

Metode (Non- Riset) menguraikan cara yang digunakan untuk menyelesaikan masalah atau persoalan masyarakat. Metode yang digunakan sebagai berikut.

1. Pendidikan Masyarakat : digunakan untuk kegiatan-kegiatan, seperti a) pelatihan semacam in-house training; b) penyuluhan yang bertujuan meningkatkan pemahaman serta kesadaran, dan sebagainya.

2. Pelatihan: digunakan untuk kegiatan yang melibatkan a) penyuluhan tentang substansi kegiatan yang disertai dengan demonstrasi atau percontohan untuk realisasinya, b) pelatihan dalam pengoperasian sistem atau peralatan, c) pembentukan kelompok wirausaha baru, d) penyediaan jasa layanan bersertifikat kepada masyarakat

3. Mediasi: digunakan untuk kegiatan yang di dalamnya pelaksana pengabdian masyarakat memposisikan diri sebagai mediator para pihak yang terkait dan bersama-sama menyelesaikan masalah yang ada dalam masyarakat

4. Simulasi Ipteks: digunakan untuk kegiatan yang karya utamanya adalah sistem informasi atau sejenisnya. Kegiatan ini ditujukan untuk menjelaskan sesuatu yang tidak dapat dilakukan secara nyata

5. Substitusi Ipteks: Digunakan untuk kegiatan yang menawarkan ipteks baru yang lebih modern dan efisien daripada ipteks lama (Ipteks berupa TTG)

Metode (Berdasarkan Riset) yang digunakan untuk memecahkan (mereduksi) masalah dan juga metode untuk menganalisis bagaimana efektifitas atau keberhasilan program. Langkah-langkah dari metode yang digunakan yaitu Service learning; Community development, atau metode/ pendekatan yang lainnya. Bagian metode ini juga menjelaskan subjek yang menjadi sasaran program pengabdian, bagaimana cara mendapatkan data, jenis data yang telah diperoleh, dan bagaimana menganalisisnya.

## **HASIL DAN PEMBAHASAN**

### **Modus Penipuan 1 : Memanfaatkan Emosional & Urgensi**

- a. Pesan Text Palsu : Email/teks palsu untuk mencuri kredensial. Contoh: "sekarang ini ada banyak maraknya pesan yang mengatas namakan pihak bank yang membutuhkan verifikasi kita dengan mengklik kode ataupun link agar bisa merampas data dan mencuri akun bank kita."
- b. Peniruan (keluarga/teman) : Saat ini banyak orang tua yang tertipu dengan hal ini ketika ditelpon oleh seseorang yang mengaku sebagai sahabat dari anak/cucu mereka. Dikarenakan adanya kekhawatiran dan ketakutan orang tua apabila terjadi sesuatu dengan keluarganya dan tidak sempat berpikir panjang. Bukan hanya itu, sekarang sudah banyak beredar akun-akun media sosial yang mengatasnamakan nama orang lain, sehingga melalui akun tersebut akan meminta sejumlah uang ataupun lainnya kepada kerabat orang yang ia gunakan identitas.

Pemerintah memiliki peran penting dalam mencegah penipuan online atau scammer melalui berbagai upaya seperti peningkatan literasi digital, penegakan hukum, dan pemblokiran situs web atau akun yang terindikasi melakukan penipuan. Selain itu, pemerintah juga dapat mendorong pembentukan kelompok swadaya masyarakat untuk meningkatkan kesadaran dan kewaspadaan masyarakat terhadap penipuan online. Berikut adalah beberapa peran pemerintah dalam mencegah penipuan online:

1. Peningkatan Literasi Digital:

Pemerintah dapat menyelenggarakan program edukasi dan pelatihan mengenai cara mengenali dan menghindari penipuan online.

Penyebaran informasi edukatif melalui berbagai media, termasuk media sosial, juga dapat dilakukan untuk meningkatkan kesadaran masyarakat.

#### 2. Penegakan Hukum:

Pemerintah perlu memperkuat penegakan hukum terhadap pelaku penipuan online, termasuk memberikan sanksi yang tegas.

Kerja sama antar lembaga pemerintah dalam bidang keamanan siber juga perlu ditingkatkan.

#### 3. Pemblokiran Situs Web dan Akun Terindikasi Penipuan:

Pemerintah dapat melakukan pemblokiran terhadap situs web, aplikasi, atau akun media sosial yang terindikasi melakukan penipuan setelah adanya laporan dari masyarakat.

Masyarakat dapat melaporkan nomor telepon atau akun yang mencurigakan melalui layanan pengaduan yang disediakan oleh pemerintah.

#### 4. Pembentukan Kelompok Swadaya Masyarakat:

Pemerintah dapat mendorong pembentukan kelompok swadaya masyarakat yang fokus pada pencegahan penipuan.

Kelompok ini dapat menjadi wadah bagi masyarakat untuk saling berbagi informasi, mengawasi lingkungan sekitar, dan melaporkan aktivitas mencurigakan.

#### 5. Pengawasan dan Perlindungan Konsumen:

Pemerintah perlu memastikan bahwa platform e-commerce dan penyedia layanan keuangan memiliki sistem keamanan yang memadai untuk melindungi konsumen. Penyediaan informasi dan layanan pengaduan yang mudah diakses oleh masyarakat juga penting untuk membantu korban penipuan. Dengan upaya-upaya tersebut, diharapkan pemerintah dapat menciptakan lingkungan digital yang lebih aman dan melindungi masyarakat dari ancaman penipuan online (Manajemen et al., 2024)

### **Modus Penipuan II: Peluang Palsu**

- a. Penipuan Investasi : Menjanjikan keuntungan tinggi, dijamin. Contoh: "Beberapa tahun yang lalu di pulau Nias, saat hebohnya aplikasi/ situs web investasi FF91 yang memberikan penawaran tertarik, dimana ketika kita menginvestasi uang kita maka akan menghasilkan uang berlipat ganda dalam beberapa hari dengan mengikuti tugas yang diberikan. Tetapi pada nyatanya setelah banyak masyarakat menginvestasikan uangnya

ke dalam situs tersebut, tiba-tiba situs tersebut tidak lagi berfungsi dan meraup semua uang masyarakat pada saat itu"

- b. **Penipuan Tawaran Pekerjaan dari Rumah** : Seperti yang kita ketahui dari media sosial, bahwa sedang banyaknya informasi kerja remote/pekerjaan yang bisa dikerjakan dari rumah dengan persyaratan minimal tamatan SMA/SMK, tetapi meminta biaya kuota masuk sebagai karyawan di awal. Contoh: "Entri data kerja dari rumah, cukup gabung di grup WhatsApp dengan membayar biaya kelas. Padahal ujung-ujungnya tidak ada pekerjaan dan nomor anda di blok"
- c. **Penipuan Link Berhadiah (Giveaway)** : Penipuan link berhadiah ini awalnya berkedok dengan adanya pihak yang mengaku sebagai tim dari artis ataupun orang besar yang sedang membagi-bagi hadiah tunai sebesar 50jt dengan mengklik link yang diberikan, padahal setelah itu media sosial facebook akan ter-hack oleh oknum tersebut. Dan melalui akun facebook yang sudah ter-hack tersebut, maka para scammer akan menyebarluaskan informasi bahwa orang tersebut sudah memenangkan giveaway. dan masyarakat yang melihat akan percaya begitu saja dan meminta link hadiah tersebut. Sehingga akan ikut terjerumus (Riti et al., 2024).



### **Strategi Pencegahan**

Menurut (Kamran & Maskun, 2021) ada beberapa strategi pencegahan yang dapat dilakukan untuk menghindari penipuan online antara lain :

1. Verifikasi Identitas : Ketika ada pesan yang meminta konfirmasi permintaan. Pastikanlah bahwa itu pesan dari sumber yang sudah resmi. Hal ini nampak pada simbol centang yang ada disudut kanan atas si pengirim
2. Kata Sandi Kuat dan Unik : Gunakan kata sandi yang kuat dan tidak mudah ditebak oleh siapapun
3. Jaringan Aman : Hindari Wi-Fi publik untuk transaksi sensitif. Karena biasanya wi-fi ditempat umum lebih mudah di setting oleh si penipu
4. Jaga Kerahasiaan PIN : Jangan pernah membagikan PIN, password, OTP, atau data pribadi lainnya kepada siapa pun, termasuk pihak yang mengaku dari perusahaan resmi. Lembaga resmi tidak akan meminta data semacam itu melalui pesan atau telepon pribadi. Jika Anda menerima pesan SMS atau pesan WhatsApp yang menyatakan Anda sebagai pemenang dalam lomba, pastikan untuk menghubungi call center atau media sosial resmi dari lembaga terkait.
5. Waspada Situs Palsu : Tips menghindari penipuan online selanjutnya adalah dengan mewaspadaai terhadap situs palsu atau phishing dan modus penipuan menggunakan fitur penerusan panggilan (call forwarding). Penipu umumnya meminta data pribadi melalui telepon, email, faks, atau media komunikasi lainnya.
6. Waspada Nomor Tak Dikenal : Jika Anda menerima pesan dari nomor yang tak dikenal atau mencurigakan, jangan langsung membalas. Lebih baik abaikan, blokir, dan laporkan nomor tersebut. Gunakan aplikasi seperti Get Contact untuk mengecek identitas pemilik nomor,

Jangan Mudah Tergiur Promosi : Waspadaai tawaran promo yang terdengar terlalu bagus untuk jadi kenyataan. Sebelum membeli, baca ulasan pembeli lain dan pastikan toko atau

penjual punya reputasi baik. Selalu gunakan sistem pembayaran resmi di platform e-commerce, jangan transfer langsung ke rekening pribadi penjual.

---

## KESIMPULAN

Dalam menghadapi banyaknya penipuan online saat ini, kita sebagai kaum mudah harus lebih aktif dalam mencari tau trik agar tidak terjebak dalam penipuan online ini, sehingga dengan kita tahu maka kita bisa mengantisipasi dan membentengi orang tua kita agar tidak tergiur dengan segala bentuk penipuan online

## DAFTAR PUSTAKA

Aan Andrew Johaness Pahajow. (2013). Pembuktian Terhadap Kejahatan Dunia Maya dan Upaya Mengatasinya Menurut Josua Sitompul, Penanganan Cyber Crime di Indonesia. Yogyakarta: Thafa Media.

Juditha, C. (2015). Pola Komunikasi Dalam Cybercrime (Kasus Love Scams) POLA KOMUNIKASI DALAM CYBERCRIME (KASUS LOVE SCAMS) COMMUNICATION PATTERNS IN CYBERCRIME (LOVE SCAMS CASE). *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika*, 6(2), 29–40.  
<https://media.neliti.com/media/publications/122582-ID-none.pdf>

Kamran, M., & Maskun, M. (2021). Penipuan Dalam Jual Beli Online: Perspektif Hukum Telematika. *Balobe Law Journal*, 1(1), 41.  
<https://doi.org/10.47268/balobe.v1i1.501>

Maharani, F. P., Taroreh, H., & Pinasang, B. (2024). Perlindungan Hukum Terhadap Korban Penipuan Online Investasi Ilegal Menurut Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik Dalam Perspektif Hukum Pidana. *Jurnal Fakultas Hukum UNSRAT*, 13(4), 12.

Manajemen, K., Waspadai, S., Kejahatan, M., Dengan, P., Linkenter, M. B., Trianurahmah, A., Fauzi, A., Tyas, E. N., Suryanto, M. A., Rizky, M., & Wibisono, P. (2024). *Analisis Ancaman Phishing Melalui Aplikasi WhatsApp: Studi*. 1(10), 190–197. <https://inovanpublisher.org/orbit>

Riti, Y. F., Teknik, F., Katolik, U., & Cendika, D. (2024). *PENYULUHAN DAN EDUKASI IDENTIFIKASI MODUS PENIPUAN MELALUI MEDIA SOSIAL BAGI MASYARAKAT*. 3(1), 245–252.

Tertibi, Y., Ayu Lestari, A., & kunci, K. (2023). Kehebatan Scammer Love Dalam Mencari Korban Ditinjau Dari Aspek Hukum Dan Psikologi. *Tahun*, 3(3), 59–67.  
[https://pusiknas.polri.go.id/detail\\_artikel/kejahatan\\_siber\\_](https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_)

Wahyuddin, Lutfiah Firdausiah Ersas, Gusti Aningsih, Taufik Hidayat, & Alem Febri

---

Sonni. (2024). Analisis Jaringan Komunikasi Penipuan Online Melalui Media Sosial Whatsapp Messenger. *Jurnal Netnografi Komunikasi*, 2(2), 33–50.  
<https://doi.org/10.59408/jnk.v2i2.27>

Undang-Undang Nomor 2 Tahun 2002 Kepolisian Negara Republik Indonesia  
Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 35 jo. Pasal 51.