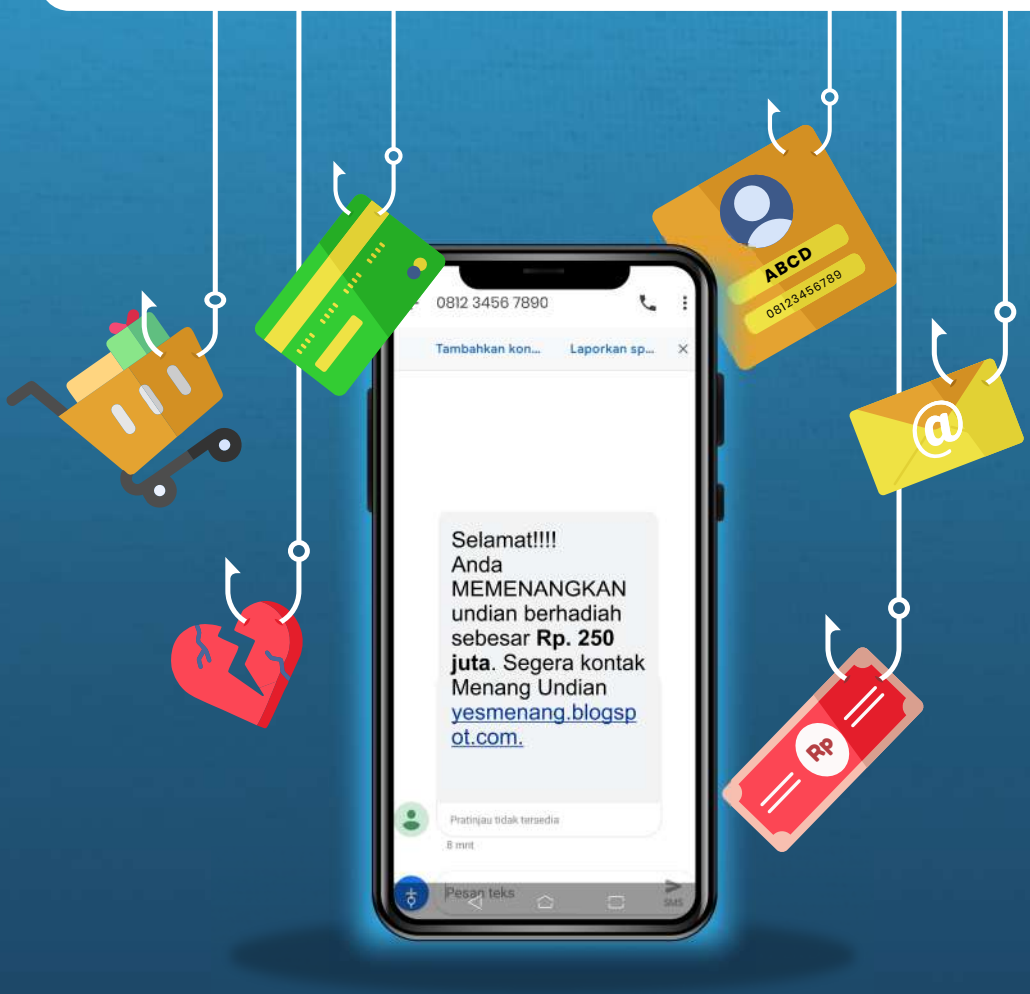
WhatsApp
CfDS CENTER FOR DIGITAL SOCIETY
UNIVERSITAS GADJAH MADA
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
DEPARTEMEN ILMU KOMUNIKASI
PROGRAM STUDI MAGISTER ILMU KOMUNIKASI
pr2media



PENIPUAN DIGITAL DI INDONESIA

MODUS, MEDIUM, DAN REKOMENDASI

Novi Kurnia – Rahayu - Engelbertus Wendratama
Zainuddin Muda Z. Monggilo - Acniah Damayanti
Dewa Ayu Diah Angendari - Firya Qurratu'ain Abisono
Irnasya Shafira – Desmalinda

WhatsApp CfDS CENTER FOR DIGITAL SOCIETY
UNIVERSITAS GADJAH MADA
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
DEPARTEMEN ILMU KOMUNIKASI
PROGRAM STUDI MAGISTER ILMU KOMUNIKASI
pr2media

PENIPUAN DIGITAL DI INDONESIA

MODUS, MEDIUM, DAN REKOMENDASI

Novi Kurnia – Rahayu - Engelbertus Wendratama
Zainuddin Muda Z. Monggilo - Acniah Damayanti
Dewa Ayu Diah Angendari - Firya Qurratu'ain Abisono
Irnasya Shafira – Desmalinda

WhatsApp CfDS CENTER FOR DIGITAL SOCIETY

UNIVERSITAS GADJAH MADA
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
DEPARTEMEN ILMU KOMUNIKASI
PROGRAM STUDI MAGISTER ILMU KOMUNIKASI

pr2media

PENIPUAN DIGITAL DI INDONESIA

MODUS, MEDIUM, DAN REKOMENDASI

Novi Kurnia – Rahayu - Engelbertus Wendratama
Zainuddin Muda Z. Monggilo - Acniah Damayanti
Dewa Ayu Diah Angendari - Firya Qurratu'ain Abisono
Irnasya Shafira – Desmalinda

PENIPUAN DIGITAL DI INDONESIA

MODUS, MEDIUM, DAN REKOMENDASI

Penulis
Novi Kurnia - Rahayu - Engelbertus Wendratama
Zainuddin Muda Z. Monggilo - Acniah Damayanti
Dewa Ayu Diah Angendari - Firya Qurratu'ain Abisono
Irnasya Shafira - Desmalinda

Penyunting
Novi Kurnia
Engelbertus Wendratama

Proofreader
Putri Laksmi Nurul Suci

Desain Sampul & Tata Letak
Mohammad Arifin

Penerbit
Program Studi Magister Ilmu Komunikasi
Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Gadjah Mada

Ukuran : 15,5 x 23 cm
Halaman: iv + 120

ISBN : 978-623-99942-2-8
E-ISBN : 978-623-99942-3-5

Cetakan Pertama: Agustus 2022

KATA PENGANTAR WHATSAPP

Internet telah menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari, sehingga menjadi penting untuk memahami pentingnya pendidikan dan fitur-fitur keamanan di dunia daring. Mengingat betapa pentingnya privasi dan keamanan pengguna kami bagi WhatsApp, kami bekerja sama dengan beberapa organisasi masyarakat sipil, kelompok industri, dan pemerintah, termasuk Kementerian Komunikasi dan Informatika (Kominfo), untuk menjalankan program literasi digital yang berkelanjutan bagi pengguna internet di berbagai penjuru Indonesia.

Pada sejumlah program yang kami jalani, kami mendengar banyak pengalaman tentang penipuan digital. Meskipun kesadaran sudah cukup tinggi di antara pengguna internet, belum banyak penelitian yang mengungkap masalah penipuan *online* tersebut beserta kerumitannya. Ketika berdiskusi dengan tim penelitian yang dipimpin oleh Dr. Novi Kurnia di Center for Digital Society Universitas Gadjah Mada (CfDS UGM), kami menemukan semangat yang sama untuk menelaah lebih lanjut topik penipuan digital, dengan harapan dapat memunculkan wawasan yang dapat mengarah pada solusi yang lebih efektif.

Sebagai bagian aktif dari ekosistem *online*, WhatsApp ingin berkontribusi di mana pun kita bisa. Kami berharap dengan dirilisnya "Riset Nasional: Penipuan Digital di Indonesia: Modus, Medium dan Rekomendasi" dapat memberikan kontribusi pemahaman yang lebih baik dan tindakan bersama oleh para pemangku kepentingan terkait dalam upaya memerangi dan memberantas penipuan digital di Indonesia. Informasi yang lekat dengan tatanan lokal seperti riset nasional ini adalah langkah awal yang sangat penting dan akan membangun fondasi yang tepat bagi organisasi publik, swasta, akademisi, dan masyarakat sipil untuk berkolaborasi dalam mencari cara untuk memecahkan masalah terkait penipuan digital bersama.

Kami mengapresiasi kinerja tim peneliti UGM sebagai lembaga penelitian dan pemikir akademis yang kredibel, yang berfokus pada upaya memajukan masyarakat digital. Kami optimistis bahwa temuan dari laporan yang telah dipikirkan dengan matang ini akan melahirkan pengetahuan dan pengembangan kebijakan yang lebih kuat serta menghadirkan program pencegahan penipuan oleh yang efektif oleh pemerintah, sektor swasta, dan organisasi masyarakat sipil.

Esther Samboh
Manajer Kebijakan Publik WhatsApp Indonesia

KATA PENGANTAR
DEKAN FISIPOL UGM

Revolusi digital telah membawa perubahan sangat mendasar di berbagai aspek kehidupan, baik dalam maknanya yang positif maupun dampak negatifnya. Secara positif perkembangan digital telah mempermudah dan mempercepat berbagai transformasi di sektor layanan publik, membuka ruang dan kesempatan transformasi ekonomi yang lebih merata, dan menyediakan arena baru bagi relasi dan kohesi sosial. Namun sejumlah kemungkinan dampak negatif juga sangat perlu dimitigasi, salah satunya adalah munculnya bentuk-bentuk kejahatan baru yang menggunakan medium *online.*

Monograf yang disusun dari riset berjudul "Penipuan Digital: Modus, Medium, dan Rekomendasi" ini, membantu kita memahami salah satu dampak negatif perkembangan digital, yaitu maraknya fenomena penipuan digital dalam beberapa tahun terakhir. Riset ini merupakan kolaborasi antara CfDS Fisipol UGM, Program Studi Magister Ilmu Komunikasi Fisipol UGM, dan PR2Media dengan dukungan dari WhatsApp. Ini merupakan kolaborasi berkelanjutan, setelah sebelumnya WhatsApp juga mendukung riset *"WhatsApp Group and Digital Literacy among Indonesian Women"* pada tahun 2018-2019 dan "Pelatihan Literasi Digital untuk Perempuan Indonesia Melawan Hoaks Pilkada" pada tahun 2020.

Hasil riset ini menunjukkan pemetaan yang komprehensif terkait dengan pengalaman berbagai kalangan masyarakat yang diwakili oleh para responden dan informan dalam menghadapi penipuan digital. Aspek-aspek yang dicakup dalam riset yang kemudian dituangkan dalam monograf ini mencakup: pesan, modus, medium, kerugian, respons, dan rekomendasi. Sebagai sebuah riset yang berorientasi pada advokasi kebijakan, monograf ini juga menawarkan sejumlah rekomendasi untuk mencegah dan menangani penipuan digital di Indonesia, baik yang bisa dilakukan oleh pemerintah selaku regulator, penyedia platform, maupun masyarakat.

Atas suksesnya pelaksanaan riset dan diterbitkannya monograf ini, saya mengucapkan selamat dan berterima kasih kepada segenap tim peneliti yang dipimpin oleh Dr. Novi Kurnia. Monograf ini akan memperkaya kajian dan diskusi terkait dengan tranformasi digital, yang juga menjadi salah satu topik *flagship* di Fisipol UGM, dan tentunya akan menginspirasi kajian-kajian selanjutnya.

Wawan Mas'udi, Ph.D.
Dekan Fisipol UGM

KATA PENGANTAR PENYUNTING BUKU

Buku berjudul "Penipuan Digital di Indonesia: Modus, Medium, dan Rekomendasi" disusun berdasarkan riset nasional berjudul sama yang dilakukan pada bulan Februari hingga Juni tahun 2022. Riset ini diawali dari keprihatinan atas semakin meningkatnya jenis penipuan digital terjadi di Indonesia. Sebagai salah satu kejahatan siber yang paling banyak terjadi, penipuan digital banyak menimbulkan korban dan berdampak pada kerugian finansial maupun non-finansial.

Agar bisa merekomendasikan solusi yang bersifat kolaboratif untuk mencegah dan menangani penipuan digital di Indonesia, riset nasional ini memetakan berbagai jenis pesan, modus, medium, kerugian, respons, dan rekomendasi yang diusulkan korban dan target penipuan digital di Indonesia.

Riset ini dilakukan atas kerja sama Center for Digital Society (CfDS) Fisipol UGM, Program Magister Ilmu Komunikasi Fisipol UGM, dan Pemantau Regulasi dan Regulator Media yang didukung oleh WhatsApp. Sebanyak 1700 responden dari 34 provinsi di Indonesia terlibat dalam survei nasional ini. Selain itu, 31 informan yang merupakan korban penipuan digital juga menjadi informan riset ini baik sebelum penyusunan instrumen survei maupun setelah terselenggaranya survei.

Atas terselenggaranya riset ini, kami mengucapkan terima kasih kepada WhatsApp sebagai pendukung utama dari penelitian yang dijalankan dalam program riset nasional berjudul "Penipuan Digital di Indonesia: Modus, Medium, dan Rekomendasi".

Kami juga sangat menghargai kontribusi dari berbagai pihak yang membantu pelaksanaan riset ini:

- Wawan Mas'udi, Ph.D. Dekan Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Gadjah Mada
- Dr. Nurhadi Susanto, Wakil Dekan Bidang Keuangan dan Sumberdaya Manusia, Fakultas Ilmu Sosial dan Ilmu Politik Universitas Gadjah Mada
- Fina Itriyati, Ph.D. Wakil Dekan Bidang Penelitian dan Pengabdian Kepada Masyarakat, Kerja sama, dan Alumni, Fakultas Ilmu Sosial dan Ilmu Politik Universitas Gadjah Mada
- Dr. Rajiyem, Ketua Departemen Ilmu Komunikasi, Fakultas Ilmu Sosial dan Ilmu Politik Universitas Gadjah Mada
- Koordinator enumator untuk 34 propinsi di Indonesia :
  - Hendra Syahputra (Aceh)
  - Yovita Sabarina Sitepu (Sumatera Utara)

- AB Sarca Putera (Sumatera Barat)
- Rozi Alamsyah (Riau)
- Pramesti Tiara Andini (Jambi)
- Desmalinda (Sumatera Selatan)
- Lisa Adhrianti (Bengkulu)
- Yohana Shera Raynardia Findi Nugraha (Lampung)
- Fatia Ramadhana (Kepulauan Bangka Belitung)
- Dewi Murni (Kepulauan Riau)
- Elisa Putriani (DKI Jakarta)
- Ratri Rizki Kusumalestari (Jawa Barat)
- Lintang Ratri Rahmiaji (Jawa Tengah)
- Whafir Pramesty (D.I. Yogyakarta)
- Frida Kusumastuti (Jawa Timur)
- Anna Agustina (Banten)
- Ni Made Ras Amanda Gelgel (Bali)
- Aurelius Rofinus Lolong Teluma (Nusa Tenggara Barat)
- Fransiska Desiana Setyaningsih (Nusa Tenggara Timur)
- Yuve Kukuh Sesar (Kalimantan Barat)
- Ghifari Syahfri Mantovani (Kalimantan Tengah)
- Sri Astuti (Kalimantan Selatan)
- Kheyene Molekandella Boer (Kalimantan Timur)
- Winona Umacina (Kalimantan Utara)
- Anastasya Patricia Killis (Sulawesi Utara)
- Zainab Syifa Alkaf (Sulawesi Tengah)
- Citra Rosalyn Anwar (Sulawesi Selatan)
- Jumrana Sukisman (Sulawesi Tenggara)
- Andi Sri Wulandari (Gorontalo dan Sulawesi Barat)
- Dzulkifli Kalla Halang (Maluku dan Maluku Utara)
- Dewi Anggraeni (Papua dan Papua Barat)
- Tim enumerator di seluruh 34 provinsi di Indonesia.

- Tim olah data stastitik survei. Lina Arifatul Hidayah
- Tim Mahasiswa Departemen Ilmu Komunikasi yang terlibat dalam riset ini:
  - Program S1 reguler : Yogama Wisnu Oktyandito, Renatta Karuna Dharani, Muhammad Fadhil Pramudya Putra, Salsabilla Amiyard Siwi
  - Program S2 : Desmalinda
  - Program S3 : Nur Imroatus
- Seluruh responden dan informan dari 34 provinsi di Indonesia.

Penyunting Buku
Novi Kurnia
Engelbertus Wendratama

RINGKASAN EKSEKUTIF

Penipuan digital adalah jenis kejahatan yang jumlah dan modusnya meningkat pesat seiring digitalisasi di Indonesia. Karena itu, pemetaan terhadap insiden, saluran, korban, kerugian, dan rekomendasi sangat penting untuk dilakukan. Survei nasional terhadap 1.700 responden laki-laki dan perempuan di 34 provinsi Indonesia yang diperkaya dengan dua *Focus Group Discussion* (FGD) bersama 20 responden terplih ini bertujuan melakukan pemetaan tersebut.

Riset ini menunjukkan tingginya kerentanan masyarakat terhadap penipuan digital, yaitu sebanyak 98,3% responden (1.671 orang) pernah menerima pesan penipuan digital, baik satu maupun lebih. Modus pesan penipuan yang paling banyak mereka terima adalah penipuan berkedok hadiah (91,2%), pinjaman ilegal (74,8%), pengiriman tautan/*link* yang berisi *malware*/virus (65,2%), penipuan berkedok krisis keluarga (59,8%), dan investasi ilegal (56%).

Medium komunikasi yang paling banyak digunakan dalam penipuan adalah jaringan seluler (SMS/telepon) (64,1%), yang sifatnya sangat mudah, murah, dan merupakan fitur mendasar pada telepon seluler sehingga jangkauannya bisa sangat luas. Medium terbanyak selanjutnya adalah media sosial (12,3%), aplikasi *chat* (9,1%), situs web (8,9%), dan email (3,8%).

Riset ini mencatat temuan memprihatinkan berupa 66,6% responden (1.132 orang) pernah menjadi korban penipuan digital. Modus penipuan dengan korban paling banyak adalah penipuan berkedok hadiah (36,9%), pengiriman tautan/*link* yang berisi *malware*/virus (33,8%), penipuan jual-beli (29,4%), situs web/aplikasi palsu (27,4%), dan penipuan berkedok krisis keluarga (26,5%).

Meski demikian, lebih dari separuh responden (50,8%) yang menjadi korban penipuan menyatakan bahwa mereka "tidak mengalami kerugian". Alasan utamanya adalah mereka telah "mengikhlaskan peristiwa itu" sebagai bagian dari "cobaan" atau "perjalanan hidup".

Kadang, mereka juga melihat kebocoran data pribadi bukan sebagai kerugian karena tidak mengalami kerugian yang langsung dirasakan. Sementara itu, korban yang menyatakan mengalami kerugian uang berjumlah 15,2% responden, yang diikuti oleh yang merasakan kerugian waktu (12%), dan kerugian perasaan (8,4%).

Dari seluruh korban penipuan tersebut, respons atau tindakan terbanyak yang mereka lakukan adalah menceritakan kepada keluarga atau teman (48,3%), tidak melakukan apa-apa (37,9%), menceritakan kepada warganet (5,3%), melaporkan kepada media sosial atau platform digital lainnya (5%), dan melaporkan kepada kepolisian (1,8%).

Meski lapor ke kepolisian hanya menjadi pilihan 1,8% responden, sebanyak 94,8% responden menganggap kepolisian dan aparat penegak hukum lainnya sebagai pihak yang paling bertanggung jawab untuk mencegah dan menangani penipuan digital, yang diikuti oleh pemerintah (92,4%), perusahaan terkait (90,6%), organisasi masyarakat sipil atau komunitas-komunitas di masyarakat (86,3%), dan perguruan tinggi (83,5%).

Sementara itu, mengenai upaya untuk mencegah dan menangani penipuan digital, rekomendasi dari para responden adalah peningkatan sistem keamanan dan perlindungan data pribadi (98%), kepastian hukum bagi penanganan penipuan digital (97,7%), publikasi kasus dan modus operandi penipuan digital terkini (97,4%), edukasi tentang keamanan digital (96,9%), ketersediaan laman dan aplikasi dari pihak berwenang untuk bisa mengecek validitas penjual (96,9%), dan kampanye publik agar warga berhati-hati dan tip cara menghindari penipuan (95,5%).

FGD dengan para korban penipuan juga mencatat rekomendasi dari mereka berupa perlunya tindakan ekstra dari otoritas, yaitu pemerintah, kepolisian, dan perbankan untuk melacak dengan cepat nomor telepon seluler, akun media sosial, dan akun bank yang terindikasi penipuan. Kemudian, mengingat dominannya pemakaian nomor seluler (melalui SMS atau panggilan telepon) dalam tindak penipuan, Kementerian Kominfo dan operator seluler perlu menertibkan penjualan nomor seluler di pasaran sehingga setiap nomor seluler yang aktif bisa dipastikan identitas pemiliknya.

Temuan riset ini akan digunakan untuk mendiskusikan aksi dengan berbagai pemangku kepentingan, sebagai referensi penyusunan *policy brief* yang diharapkan menjadi awal aksi kolaborasi untuk mencegah dan menangani penipuan digital.

DAFTAR ISI

Kata Pengantar WhatsApp 1
Kata Pengantar Dekan Fisipol UGM 2
Kata Pengantar Penyunting Buku 3
Ringkasan Eksekutif 5
Daftar Isi 7
Daftar Gambar 10

Bab 1. Urgensi Riset Nasional Tentang Penipuan Digital di Indonesia 14
Latar Belakang 15
Tinjauan Pustaka 17
- Terminologi Penipuan Digital 17
- Ragam Penipuan Digital 19
- Medium Penipuan Digital 24
- Kerugian Penipuan Digital 24
- Model Pencegahan dan Penanganan Penipuan Digital 25

Metode Riset 30
Sistematika Buku 36

Bab 2. Profil Responden dan Informan 38
Pengantar 39
Jenis Kelamin Responden 39
Usia Responden 40
Tingkat Pendidikan Responden 41
Status Responden 42
Jenis Pekerjaan Responden 42
Pendapatan Rata-rata Per Bulan 43
Provinsi Tempat Tinggal 44
Ragam Kegiatan Daring 44
Profil Peserta *Focus Group Discussion* 50
- Profil Peserta FGD Awal 50
- Profil Peserta FGD Akhir 51

Bab 3. Pesan dan Medium Penipuan Digital 55
Pengantar 55
Pesan Penipuan Digital 55
Jenis Pesan Penipuan Digital yang Diterima 55
Jenis Pesan Penipuan yang Diterima Berdasarkan Gender 57
Ragam Pengalaman Penerima Pesan Penipuan 58
Medium Penipuan Digital 60
Jaringan Selular (SMS/Telepon) 62
Media Sosial 63
Aplikasi *Chat* 65
Situs Web 66
Email 67
Lokapasar 68
Game 69
Dompet Elektronik *(e-wallet)* 71

Bab 4. Korban Penipuan Digital 74
Pengantar 75
Korban dan Proses Menjadi Korban Penipuan Digital 75
Modus Penipuan Digital dan Korbannya 78
Korban Penipuan Digital dan Usia 78
Korban Penipuan Digital dan Pendapatan 83
Korban Penipuan Digital dan Tingkat Pendidikan 84

Bab 5. Kerugian Penipuan Digital 86
Pengantar 87
Menjadi Korban Tapi Tidak Ada Kerugian 88
Kerugian Uang 89
Kerugian Waktu 90
Kerugian Perasaan 91
Kebocoran Data Pribadi 93
Kerugian Barang 94
Kerugian Fisik 95

Bab 6. Respons Korban Penipuan Digital 96
Pengantar 97
Menceritakan Kepada Keluarga atau Teman 98
Tidak Melakukan Apa-apa 99
Menceritakan Kepada Warganet 100
Melaporkan Kepada Kepolisian 101
Melaporkan Kepada Lembaga/Otoritas Terkait 102
Melaporkan Kepada Lembaga Pemerintah atau Kementerian 103
Melaporkan Kepada Lembaga Bantuan Hukum 104
Melaporkan Kepada Lembaga Perlindungan Warga atau Konsumen 105

Bab 7. Rekomendasi Pencegahan dan Penanganan Penipuan Digital 106
Pengantar 107
Pencegahan Penipuan Digital 107
Penanganan Penipuan Digital 112
Pihak Terpercaya Memberikan Informasi Pencegahan 113
Pihak yang Dianggap Responden Bertanggung Jawab dalam Mencegah dan Menangani Penipuan Digital 114
Rekomendasi Pencegahan Menurut Korban Penipuan Digital 116
Rekomendasi Penanganan Menurut Korban Penipuan Digital 118

Bab 8. Penutup 122
Pengantar 123
Pemetaan Penipuan Digital di Indonesia 123
Rekomendasi Pencegahan dan Penanganan Penipuan Digital di Indonesia 124
- Penertiban Nomer Seluler 125
- Kepastian Hukum dalam Tindak Lanjut Laporan Penipuan Digital 126
- Perlindungan Data Pribadi dan Keamanan Siber 127
- Sosialisasi dari Otoritas 127
- Kampanye Literasi Digital dari Non-otoritas 128

Daftar Pustaka 129

DAFTAR GAMBAR

Gambar 1.1. Ragam Penipuan Digital 20
Gambar 1.2. Pendekatan *Multi-Layered* untuk *Phishing* 28
Gambar 1.3. Sebaran Jumlah Responden Per Provinsi 31
Gambar 1.4. Modus Penipuan Digital 33
Gambar 1.5. Medium Penipuan Digital 34
Gambar 1.6. Sistematika Buku 36
Gambar 2.1. Jenis Kelamin Responden 39
Gambar 2.2. Jumlah Responden Berdasarkan Generasi Usia 40
Gambar 2.3. Tabulasi Silang Generasi Usia dan Jenis Kelamin 41
Gambar 2.4. Tingkat Pendidikan Responden 41
Gambar 2.5. Status Responden 42
Gambar 2.6. Pekerjaan Utama Responden 43
Gambar 2.7. Pendapatan Rata-rata Per Bulan Responden 43
Gambar 2.8. Provinsi Tempat Tinggal Responden 44
Gambar 2.9. Kegiatan Daring yang Paling Menyita Waktu 45
Gambar 2.10. Kegiatan Daring yang Paling Menyita Waktu antar Generasi Usia 47
Gambar 3.1. Persentase Responden yang Pernah Menerima Pesan Penipuan 55
Gambar 3.2. Jenis Penipuan Digital yang Diterima 56
Gambar 3.3. Pesan Penipuan yang Diterima Berdasarkan Gender 57
Gambar 3.4. Persentase Penerimaan Pesan yang Diterima Berdasarkan Gender 57
Gambar 3.5. Delapan Medium yang Digunakan Penipu untuk Mengirim Pesan Penipuan 60
Gambar 3.6. Pesan/Modus Penipuan dan Medium yang Paling Sering Digunakan 61
Gambar 3.7. Urutan Modus Operandi yang Dilakukan Melalui Jaringan Seluler (SMS/Telepon) 62
Gambar 3.8. Urutan Modus Operandi yang Dilakukan Melalui Media Sosial 64
Gambar 3.9. Urutan Modus Operandi yang Dilakukan Melalui Aplikasi *Chat* 65

Gambar 3.10. Urutan Modus Operandi yang Dilakukan Melalui Situs Web 66
Gambar 3.11. Urutan Modus Operandi yang Dilakukan Melalui Email 67
Gambar 3.12. Urutan Modus Operandi yang Dilakukan Melalui Lokapasar 68
Gambar 3.13. Urutan Modus Operandi yang Dilakukan Melalui *Game* 70
Gambar 3.14. Urutan Modus Operandi yang Dilakukan Melalui Dompet Elektronik 71
Gambar 4.1. Korban Penipuan Digital 75
Gambar 4.2. Modus Penipuan Digital dan Korbannya 77
Gambar 4.3. Korban Penipuan Digital Berdasarkan Usia 79
Gambar 4.4. Korban Penipuan Digital Berdasarkan Kelompok Usia 80
Gambar 4.5. Korban Penipuan Digital Berdasarkan Pendapatan 83
Gambar 4.6. Korban Penipuan Digital Berdasarkan Pendidikan 84
Gambar 5.1. Jumlah Responden yang Pernah Menjadi Korban Penipuan Digital (N=1.132) 87
Gambar 5.2. Jenis Penipuan Digital dan Korban yang Tidak Merasa Tidak Ada Kerugian (N=1.132) 88
Gambar 5.3. Jenis Penipuan Digital dan Kerugian Uang (N=1.132) 89
Gambar 5.4. Jenis Penipuan Digital dan Kerugian Waktu (N=1.132) 91
Gambar 5.5. Jenis Penipuan Digital dan Kerugian Perasaan (N=1.132) 92
Gambar 5.6. Jenis Penipuan dan Kebocoran Data Pribadi (N=1.132) 93
Gambar 5.7. Jenis Penipuan Digital dan Kerugian Barang (N=1.132) 94
Gambar 5.8. Jenis Penipuan dan Kerugian Fisik (N=1.132) 95
Gambar 6.1. Respons Korban Penipuan Digital (N=1.132) 97
Gambar 6.2. Menceritakan Kepada Keluarga atau Teman dan 5 Modus Penipuan Digital Terbanyak (N=1.132) 98
Gambar 6.3. Tidak Melakukan Apa-apa dan 5 Modus Penipuan Digital Terbanyak (N=1.132) 99

Gambar 6.4.	Menceritakan Kepada Warganet dan 5 Modus Penipuan Digital Terbanyak (N=1.132)	**100**
Gambar 6.5.	Melaporkan Kepada Polisi dan 5 Modus Penipuan Digital Terbanyak (N=1.132)	**101**
Gambar 6.6.	Jumlah Laporan Penipuan Online Per Tahun dari Kepolisian Republik Indonesia	**102**
Gambar 6.7.	Melaporkan Kepada Lembaga/Otoritas Terkait dan 5 Modus Penipuan Digital Terbanyak (N=1.132)	**103**
Gambar 6.8.	Melaporkan Kepada Lembaga Pemerintah atau Kementerian dan Modus Penipuan Digital (N=1.132)	**103**
Gambar 6.9.	Melaporkan Kepada Lembaga Bantuan Hukum dan Modus Penipuan Digital (N=1.132)	**104**
Gambar 6.10.	Melaporkan Kepada Lembaga Perlindungan Warga atau Konsumen (N=1.132)	**105**
Gambar 7.1.	Program Pencegahan Penipuan Digital (N=1.700)	**108**
Gambar 7.2.	Program Menangani Penipuan Digital (N=1.700)	**112**
Gambar 7.3.	Pihak Terpercaya Memberikan Informasi Pencegahan (N=1.700)	**114**
Gambar 7.4.	Pihak yang Bertanggung Jawab untuk Mencegah dan Menangani Penipuan Digital (N=1.700)	**115**
Gambar 7.5.	Rekomendasi Pencegahan Menurut Korban Penipuan Digital (N=1.132)	**116**
Gambar 7.6.	Perbandingan Rekomendasi Pencegahan Penipuan Digital	**117**
Gambar 7.7.	Rekomendasi Penanganan Menurut Korban Penipuan Digital (N=1.132)	**118**
Gambar 7.8.	Perbandingan Rekomendasi Penanganan Penipuan Digital	**119**
Gambar 8.1.	Generasi yang Paling Sering Menjadi Korban dan Modus yang Menyertai	**124**

1

URGENSI RISET NASIONAL TENTANG PENIPUAN DIGITAL DI INDONESIA

PENDAHULUAN: PENTINGNYA RISET NASIONAL PENIPUAN DIGITAL DI INDONESIA

LATAR BELAKANG

Penipuan digital merupakan kejahatan siber yang paling sering ditemui dan menjadi persoalan global (Astuty, 2021; Button et al., 2014). Penipuan digital juga sering disebut dengan penipuan *online* (*online scam/fraud*) dan penipuan siber (*cyber scam/fraud*). Laporan riset ini menggunakan penipuan digital digunakan karena untuk konteks Indonesia, beragam penipuan tak hanya terjadi melalui internet atau secara daring, tapi juga melalui perangkat seluler yang tak terhubung dengan jaringan internet.

Menurut Puram dkk. (2011) terdapat berbagai variasi penipuan digital seperti pengelabuan *(phishing),* penipuan lotre *(lottery scam)*, penipuan video *(video scams)*, pencurian identitas *(identity theft)*, dan menakut-nakuti *(scareware).* Sementara itu, Button dkk. (2014) menyebutkan ragam penipuan digital lainnya seperti penipuan berkedok asmara *(romance scams)*, penipuan berbahaya *(malicious spams)*, penipuan berkedok lowongan pekerjaan *(employment scams)*, dan penipuan berkedok investasi *(investment scams)*. Berbagai jenis penipuan tersebut disampaikan kepada korban atau calon korban melalui berbagai saluran seperti pesan pendek (SMS), pesan melalui aplikasi percakapan maupun platform sosial lainnya termasuk media sosial, email, telepon, situs web, lokapasar (*market place*), dan berbagai platform digital lainnya.

Dalam laporan yang dikeluarkan oleh Truecaller Insights Report 2020 (dalam Kumparan.com, 2021), Indonesia menjadi negara berperingkat keenam di dunia dengan penipuan melalui telepon terbanyak. Sementara itu, berdasarkan data patrolisiber.id, selama tahun 2021, terdapat 15.152 kasus kejahatan siber yang diadukan di portal milik Kepolisian Republik Indonesia tersebut, dengan penipuan digital menjadi kasus terbanyak, yakni 4.602 kasus (Dihni, 2021).

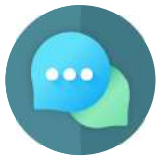
Kajian lain yang dilakukan oleh CfDS (2020) menunjukkan jenis penipuan digital lainnya yakni penipuan uang muka (*advance-fee scam*) yang banyak terjadi pada tahun 2013 hingga 2017 yang melibatkan pencurian data pribadi di ruang digital. Sementara itu, kajian lain mengenai penipuan digital di Indonesia dilakukan oleh Judhita (2015), yang menemukan bahwa penipuan berkedok asmara sebagai salah satu kejahatan siber yang paling banyak dialami perempuan Indonesia. Jenis penipuan yang melibatkan perasaan tersebut ternyata tidak hanya menyebabkan kerugian perasaan semata tapi juga kerugian finansial yang besar

Tak hanya melihat jenis dan kerugian penipuan digital, terdapat pula kajian mengenai penipuan digital dari perspektif hukum. Untuk Indonesia, salah satunya dilakukan oleh Rahmanto (2018) mengenai penegakan hukum terhadap tindak pidana penipuan berbasis transaksi elektronik yang masih mengalami banyak hambatan. Beberapa hambatan tersebut adalah perbedaan pendapat dalam menafsirkan regulasi, kemampuan penyidik, kesadaran dan perhatian masyarakat, terbatasnya personel tenaga ahli, lemahnya pengawasan pemerintah, dan kendala prosedural Undang-Undang Informasi dan Transaksi Elektronik.

Sejumlah data dan kajian di atas menunjukkan bahwa penipuan digital merupakan kejahatan yang sangat mengancam masyarakat Indonesia di era digital ini, yang tak hanya menimbulkan kerugian finansial dan psikologis tapi juga pelanggaran data pribadi. Berbagai faktor bisa diasumsikan mempengaruhi banyaknya dan beragamnya kasus penipuan digital dewasa ini. Pertama, kompetensi pengguna media dalam mengenali, mencegah, dan melawan penipuan digital. Kedua, penegakan hukum dan regulasi pencegahan yang kurang kuat. Ketiga, moderasi konten dan standar komunitas dari beragam platform digital yang belum bisa dimanfaatkan secara maksimal untuk mencegah dan menangani penipuan digital.

Meskipun demikian, belum ada kajian yang komprehensif dan nasional mengenai penipuan digital di Indonesia. Riset berskala nasional dibutuhkan untuk memetakan insiden, medium, dampak, dan respons korban penipuan digital di Indonesia, sekaligus menawarkan rekomendasi untuk mencegah dan menangani permasalahan tersebut.

Riset mengenai penipuan digital berskala nasional pertama di Indonesia ini berupaya menjawab beberapa pertanyaan penting:



Pesan Penipuan Digital
Apa saja jenis pesan atau modus penipuan digital yang diterima oleh masyarakat?

Medium Penipuan Digital
Medium apa yang biasa digunakan untuk menyampaikan pesan penipuan digital?

Korban Penipuan Digital
Jenis penipuan digital apa yang paling banyak memakan korban?

Dampak Penipuan Digital
Kerugian apa saja yang dirasakan oleh korban penipuan digital?

Keamanan Digital Korban Penipuan Digital
Respons apa yang dilakukan oleh korban penipuan digital? Pemangku kepentingan mana yang dipercaya oleh korban penipuan digital?

Rekomendasi Mencegah dan Menangani Penipuan Digital
Apa saja yang disarankan oleh korban penipuan digital untuk mencegah dan menangani penipuan digital di Indonesia? Siapa saja pemangku kepentingan yang dianggap bisa melakukannya?

TINJAUAN PUSTAKA

Terminologi Penipuan Digital

Penipuan digital adalah salah satu kejahatan siber yang banyak didiskusikan di berbagai kajian terutama terkait keamanan digital maupun literasi digital. Penggunaan terminologi penipuan digital pun beragam seperti penipuan *online* dan penipuan siber. Pada dasarnya istilah-istilah tersebut memiliki arti dan maksud yang sama yaitu merujuk pada penipuan yang memanfaatkan medium dan perangkat komunikasi digital.

Istilah penipuan digital misalnya digunakan oleh Cross et al. (2014), yang mengatakan bahwa pada dasarnya penipuan terjadi ketika seseorang menggunakan internet untuk menyediakan dana atau informasi pribadi yang menanggapi penipuan, pemberitahuan, penawaran atau permintaan, yang selanjutnya menyebabkan korban mengalami kerugian finansial atau non-finansial.

Sementara itu, Kurnia dkk. (2022) mendefinisikan penipuan digital sebagai penggunaan layanan internet atau *software* dengan akses internet untuk menipu atau mengambil keuntungan dari korban, misalnya uang dan mencuri informasi atau identitas pribadi.

Kurnia dkk. (2022) juga menggunakan istilah penipuan digital sebagai penggunaan layanan internet atau *software* dengan akses internet dengan tujuan untuk mengelabui calon korban misalnya dengan memanfaatkan kebocoran atau mencuri data pribadi. Biasanya korban terperangkap dalam penipuan karena lengah sehingga bisa diperdaya pelaku yang bertujuan mendapatkan beragam keuntungan berupa uang maupun harta material lainnya. Sedangkan istilah *cyber frauds and scams* (penipuan siber) dijelaskan oleh Button dan Cross (2017) dalam bukunya *Cyber Frauds, Scam And Their Victims* sebagai skema penipuan yang berusaha untuk menipu seseorang dalam bentuk uang dan/atau informasi pribadi secara tidak etis dan mungkin menjadi masalah sipil atau pidana juga. Buku itu juga menyebutkan salah satu skema penipuan yang paling kejam adalah pencurian identitas (*identity theft*) yang mana penipu menggunakan metode *phishing* untuk memancing korban lewat dua cara, pertama menggunakan email palsu dari organisasi yang sah (seperti bank, telepon /penyedia layanan internet) untuk menipu pelanggan agar menghasilkan informasi pribadi *(cyber-enabled),* sedangkan yang kedua menggunakan email untuk mendistribusikan *malware* ke komputer korban untuk memungkinkan pelaku mendapatkan akses ke detail pribadi korban yang disimpan di komputer atau jaringan.

Sementara itu, definisi penipuan digital digunakan dalam modul *Aman Bermedia Digital* (2021) yang diterbitkan oleh Kementerian Kominfo, Japelidi, dan Siberkreasi. Modul ini menyebutkan bahwa penipuan digital merupakan pemanfaatan aplikasi atau laman internet untuk menipu korban dengan berbagai modus seperti penjualan barang, identitas pelaku usaha atau konsumen, dan ketidaksesuaian barang atau produk yang diterima dengan yang dipesan (Astuty, 2021).

Berdasarkan beragam terminologi penipuan digital di atas, riset ini menggunakan istilah penipuan digital yang didefinisikan sebagai beragam jenis penipuan yang terjadi di dalam jaringan internet atau seluler baik melalui SMS maupun telepon.

Ragam Penipuan Digital

Dilihat dari jenisnya, Smith (2010) menggolongkan penipuan digital ke dalam dua kelompok utama yaitu:

Computer-assisted
Penipuan yang sudah ada sebelum internet dan kemudian tumbuh dan berkembang akibat adanya internet

sumber foto: informasiokkay.com

Computer-oriented
Penipuan yang baru ada usai kelahiran internet

sumber foto: spionase-news.com

Lebih jauh, Smith (2010) membagi lagi penipuan *computer-oriented* menjadi tiga kelompok penipuan:

1 ***Syntactic* (teknis)**
Penipu mengeksploitasi kelemahan-kelemahan teknis untuk mengambil data pribadi lewat *malware* seperti virus, *keylogger, worms, spyware,* dan virus trojan dan sebagainya.

2 ***Semantic (social engineering)***
Individu dikelabui untuk memberikan informasi pribadinya, umumnya lewat *phishing* (laman situs palsu dan surel spam), SMS-ing (pesan singkat), *social phishing* (media sosial), dan *vishing* (lewat telepon), dan *blended* (keduanya).

3 Gabungan dua jenis di atas dan biasanya melibatkan modus berupa permasalahan yang diciptakan pada komputer korban lalu penipu menawarkan "solusi" dengan imbalan tertentu seperti uang atau informasi pribadi (Button et al., 2014)

Bentuk ketiga ini umumnya dipakai untuk mengumpulkan informasi pribadi yang kemudian dijual dan digunakan untuk melakukan *mass marketing scams*, yaitu penipuan yang dilakukan secara massal tanpa dirancang secara spesifik untuk korban-korban tertentu.

Penipuan digital telah menjadi tantangan besar di banyak negara dengan penetrasi internet yang tinggi. Beragamnya modus dan medium penipuan digital menjadi objek penelitian di berbagai disiplin ilmu (Dam et al., 2020; Cross et al., 2014; Puram et al., 2011). Berdasarkan ketiga kajian tersebut, terdapat 14 jenis penipuan digital sebagai tampak dalam Gambar 1.1.

Gambar 1.1. Ragam Penipuan Digital

Sumber: dikompilasi dari Dam et. Al, 2020; Cross et. Al, 2014; Puram et. Al, 2011

Phishing

yakni tindakan penipuan dengan mencuri informasi penting dengan mengarahkan korban untuk masuk ke halaman/situs palsu yang bertujuan untuk menjebak korban. Pada umumnya, kejahatan ini menargetkan layanan *streaming* berbayar, perbankan, *e-commerce,* dan UMKM.

Scam

yakni penipuan yang biasanya bertujuan untuk mendapatkan uang dengan cara menipu atau membohongi orang lain. Biasanya terjadi melalui kontak komunikasi dengan aplikasi *chat,* telepon, dan lain-lain.

Account take over

yakni penipuan pengambilalihan akun secara tiba-tiba dan korban biasanya langsung merasakan dampaknya dalam sekejap.

Social engineering

yaitu tindak kejahatan yang dilakukan dengan memanfaatkan interaksi dengan manusia. Penipu akan menggunakan manipulasi psikologis untuk menipu targetnya agar melakukan kesalahan keamanan digital.

Share login info

yaitu penipuan dengan mencuri informasi sensitif terkait akun (PIN, OTP, dan *password*).

Share card info

yaitu penipuan dengan mencuri informasi data kartu, baik nomor kartu atau kode OTP dari bank penerbit. Modus yang paling umum dilakukan adalah dengan menghubungi korban dengan mengatasnamakan bank atau instasi terkait yang lainnya.

ID theft

yaitu penipuan dengan mencuri kartu identitas korban. Lalu identitas tersebut akan digunakan untuk mendaftarkan akun di suatu platform dengan identitas orang lain.

Typosquatting

yaitu penipuan dengan mendaftarkan domain suatu laman yang sangat mirip dengan laman yang sudah ada, tapi namanya sedikit berbeda dengan nama laman yang asli (seperti orang yang sedang melakukan *typo* atau salah ketik). Domain ini kemudian digunakan untuk menipu pengguna internet bahwa mereka sedang berselancar di laman situs yang mereka tuju.

Pharming

yaitu penipuan yang melibatkan pengondisian sistem komputer korban lewat *hacking, malware,* atau *software* yang membawa korban ke laman palsu di mana mereka diminta untuk memasukkan data mereka.

Skimming

yaitu penipuan di mana informasi pribadi korban di dalam kartu elektronik (seperti kartu kredit) diambil melalui alat yang secara diam-diam disematkan ke mesin pembaca kartu.

Malware

yaitu *software* penyusup seperti halnya virus yang di-*install* di komputer untuk mengalihfungsikan program ataupun dokumen.

Lottery Scams

yaitu korban mendapatkan surel dari suatu sumber yang meyakinkan bahwa korban telah memenangkan hadiah dari suatu organisasi dan untuk mendapatkan hadiah tersebut, korban harus membalas surel tersebut dengan informasi tertentu.

Video Scams

yaitu proses penipuan dengan meminta korban untuk menonton suatu video yang telah terinfeksi virus. Ketika korban mencoba untuk menonton video, mereka diinstruksikan untuk mengunduh suatu *codec* untuk menontonnya.

Video ini biasanya memilki judul yang sangat menggoda sehingga korban mau tidak mau harus mengunduh *codec* tersebut yang merupakan suatu *malware* yang mengintai seluruh aktivitas di komputer korban.

Scareware
yaitu program penyusup yang didesain untuk menipu pengguna untuk membeli dan mengunduh berbagai *software* yang berbahaya seperti antivirus palsu.

Tak hanya 14 jenis penipuan digital sebagaimana terdapat dalam Gambar 1.1, Cross dkk. (2014) juga menuliskan jenis-jenis baru dari penipuan digital:

Spearphising
pesan *spam* yang sangat menargetkan korban

SMShing
pencurian data pribadi yang didapatkan lewat SMS

Koobface
koobface di media sosial; yaitu korban dikirimi pesan-pesan yang mengandung virus di media sosial.

Vishing
data pribadi yang didapatkan lewat gawai

Keylogging Viruses
virus-virus yang secara spesifik mendapatkan detail *login* atau *password* akun korban yang kemudian dapat digunakan atau dijual.

Social Phishing
di mana pelaku mendapatkan kepercayaan individu dan mengakses daftar teman mereka atau pelaku mendapatkan akses tidak diizinkan ke akun pengguna untuk mengirimkan pesan *spam* ke kontak yang dimiliki pemilik akun tersebut.

Medium Penipuan Digital

Tak hanya jenis penipuan digital yang semakin beragam, medium yang digunakan untuk melancarkan berbagai jenis penipuan digital sangatlah beragam. Menurut Pusparisa (2020), Kepolisian Republik Indonesia mencatat bahwa dari 7.047 kasus penipuan digital yang dilaporkan, sebagian besar di antaranya terjadi melalui media sosial dengan modus yang sangat beragam.

Selain media sosial, selama tahun 2021, Yayasan Lembaga Konsumen Indonesia (YLKI) juga mencatat dari 535 kasus yang diadukan konsumen, 22,4% aduan berasal dari konsumen pinjaman *online* (pinjol), terutama terkait cara penagihan dan keberadaan pinjol ilegal. Selanjutnya, 16,6% aduan berasal dari konsumen belanja *online.* Pada 2021, data ini meningkat 33% dari total aduan tahun sebelumnya (Pahlevi, 2022).

Kerugian Penipuan Digital

Dampak yang ditimbulkan dari penipuan digital juga telah dibahas dalam berbagai studi. Badawi (2021) menjelaskan bahwa dampak dari penipuan digital bagi para korban mencakup kerugian keuangan, kebocoran data pribadi dan informasi sensitif lainnya, serta turunnya kepercayaan terhadap layanan yang disediakan oleh internet.

Komisi Eropa (2020) dalam survei mereka menjelaskan bahwa sebagian besar korban yang terkena penipuan merasakan dampak negatif seperti menderita kerugian emosional atau fisik (79%) dan menderita kerugian finansial (24%).

Korban yang mengalami penipuan dalam dua tahun terakhir digambarkan lebih relatif berhati-hati dalam perilaku *online/offline* dibandingkan dengan mereka yang tidak menjadi korban—hal ini mungkin karena perubahan perilaku yang disebabkan oleh penipuan.

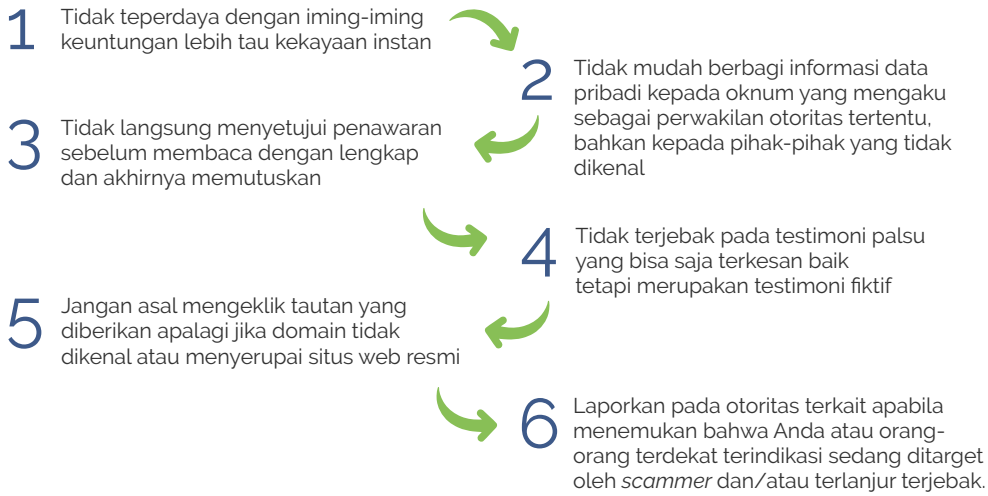
Sementara itu, Puram dkk. (2011) berargumen bahwa penipuan digital menganggu dan merusak kesenangan orang dalam berinternet. Mereka juga menuliskan bahwa penipuan digital sangatlah mirip dengan penipuan di dunia nyata, di mana korban ditipu untuk memberikan informasi pribadi dan rahasia akibat tergiur oleh suatu insentif tertentu.

Perbedaan antara penipuan di dunia nyata dan penipuan digital adalah kecepatan dari penipuan digital jauh lebih tinggi dengan kerugian yang jauh lebih merugikan.

Model Pencegahan dan Penanganan Penipuan Digital

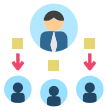
Berbagai literatur yang mengkaji soal penipuan digital juga telah memberikan berbagai rekomendasi untuk mencegah dan menangani kasus-kasus penipuan digital. Puram dkk. (2011) menuliskan bahwa langkah utama untuk mencegah penipuan digital adalah dengan selalu waspada ketika menerima pesan-pesan yang menjurus ke arah penipuan dengan mengkritisi secara logis konten dari pesan-pesan tersebut.

Lottery scams dapat dihindari dengan mengkritisi bahwa tidak ada undian yang memberikan hadiah besar tanpa mendaftar terlebih dahulu. Jenis penipuan lainnya dapat dihindari dengan cara yang sama. Sementara surel penipuan dari institusi yang mengaku sebagai bank dapat dihindari dengan menyadari bahwa bank tidak akan meminta data pribadi nasabah, dan jika terdapat keraguan akan keaslian surel apapun, semua orang dapat mengonfirmasi dengan bank terkait.



Sementara itu, di Australia, Button dkk. (2014) merekomendasikan pencegahan penipuan digital dengan memberikan pendidikan ke publik dan pemberikan peringatan kepada publik secara reguler tentang bahaya *scam,* jangan percaya pesan dari orang yang tidak dikenal tanpa melakukan verifikasi, jangan terburu mengambil keputusan, dan segera menutup laman yang tampak mencurigakan.

Sedangkan Cross dkk. (2014) merekomendasikan sepuluh hal yang perlu dilakukan otoritas dalam menyediakan layanan penanganan dan pencegahan, yaitu:

1.  Satu pekerja (orang) untuk setiap kasus
2.  Informasi terbaru mengenai kelangsungan kasus tersebut
3.  Penyedia layanan yang menggunakan pendekatan yang bersimpati kepada korban
4.  Staf yang terlatih dalam menangani korban
5.  Informasi yang jelas untuk diberikan ke pengguna internet
6.  Asistensi dalam restitusi dan kompensasi
7.  Pelayanan yang bertujuan untuk tidak membuat korban menjadi korban lagi
8.  Memberikan pendidikan bagi komunitas mengenai penipuan dan dampaknya
9.  Memberikan keterampilan bagi anggota komunitas untuk mempersiapkan mereka melawan penipu digital
10.  Memberdayakan korban sebagai "penyintas" lewat pemberdayaan diri.

Australia juga telah memiliki pusat pelaporan terpadu bernama Scamwatch yang tujuan utamanya adalah membantu masyarakat mengenali penipuan dan menghindarinya. Lembaga ini dijalankan oleh Komisi Konsumen dan Kompetisi Australia (*Australian Competition and Consumer Commission*—ACCC). Lembaga ini juga mengumpulkan data mengenai penipuan yang kemudian digunakan untuk menginformasikan masyarakat Australia mengenai berbagai macam penipuan yang beredar di Australia.

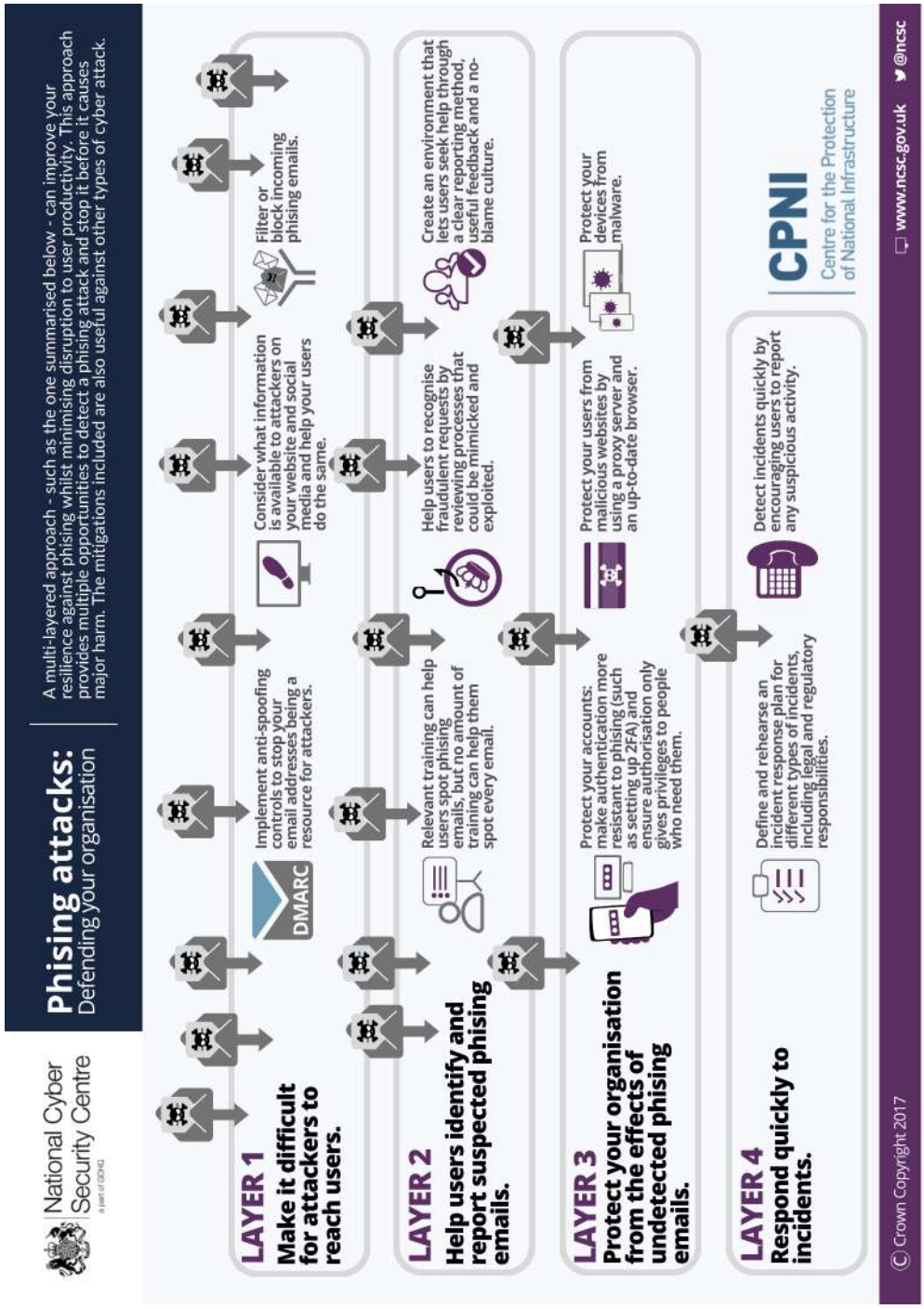
Di Inggris Raya, pemerintah telah mengeluarkan dan merevisi Undang-Undang Keamanan Daring (*Online Safety Bill*) yang mereformasi regulasi pengiklanan barang dan jasa di ranah daring yang memperkuat regulator untuk menangani iklan-iklan yang merugikan, ofensif, dan menyesatkan

serta mengharuskan platform media sosial populer dan mesin pencarian untuk mencegah iklan-iklan berbayar dari iklan palsu di platform mereka.

Di Inggris Raya, pemerintah telah mengeluarkan dan merevisi Undang-Undang Keamanan Daring (*Online Safety Bill*) yang mereformasi regulasi pengiklanan barang dan jasa di ranah daring yang memperkuat regulator untuk menangani iklan-iklan yang merugikan, ofensif, dan menyesatkan serta mengharuskan platform media sosial populer dan mesin pencarian untuk mencegah iklan-iklan berbayar dari iklan palsu di platform mereka. Pemerintah Inggris Raya juga tengah melakukan konsultasi untuk memperkuat peraturan bagi industri pengiklanan *online.* Mereka juga meningkatkan pengawasan terhadap iklan-iklan yang dapat berujung kepada penipuan (Departemen Digital, Budaya, Media dan Olahraga Inggris Raya, 2022).

Sementara secara khusus mengenai *phishing,* Pusat Keamanan Siber Nasional (*National Cyber Security Centre*, 2018) Inggris Raya mengeluarkan empat lapis pertahanan dari *phishing* yang terdiri dari: 1) menyusahkan penyerang untuk mencapai pengguna akun; 2) membantu mengidentifikasi dan melaporkan surel *phishing;* 3) melindungi organisasi Anda dari dampak yang dibawa surel *phishing* yang tidak terdeteksi, dan 4) respons cepat terhadap insiden yang terjadi. Secara lebih spesifik, pendekatan berlapis untuk pertahanan dari *phishing* ini dapat dilakukan dengan cara sebagai berikut:

Gambar 1.2. Pendekatan *Multi-Layered* untuk *Phishing*



Sumber: Department for Digital, Culture, Media & Sport, Home Office (2020, March 8)

Perlu diketahui bahwa Inggris Raya juga memiliki otoritas khusus yang menangani penipuan digital, yakni Action Fraud yang merupakan pusat pelaporan penipuan dan kejahatan siber bagi masyarakat Inggris, Wales, dan Irlandia Utara. Layanan ini diluncurkan oleh Polisi London dan Badan Intelijen Penipuan Nasional (*National Fraud Intelligence Bureau*) yang bertanggung jawab atas penilaian laporan untuk memastikan laporan masyarakat bisa ditindaklanjuti secara memadai.

Di Amerika Serikat, Komisi Perdagangan Federal (Federal Trade Comission, 2019) juga telah mengeluarkan berbagai regulasi yang bertujuan mendorong masyarakat untuk menyadari dan menghindari berbagai penipuan seperti halnya *phishing* (Federal Trade Commision Consumer Advice, n.d.), *romance scam* (Jhaveri, 2015), dan pesan singkat yang merupakan *spam* (Federal Trade Commision Consumer Advice, n.d.). Seperti halnya Amerika Serikat, Departemen Urusan Dalam Negeri Selandia Baru (*Department of Internal Affairs*) juga telah mengeluarkan halaman khusus untuk memberikan pengertian mengenai penipuan digital ke masyarakatnya.

Di Indonesia, rekomendasi pencegahan dan penanganan penipuan digital lebih banyak digunakan sebagai materi literasi digital terutama dalam membangun ketangguhan masyarakat untuk menjaga keamanan digital. Dalam modul Aman Digital (Astuty, 2021), selain dijelaskan cara-cara mengenali ciri penipuan, pembaca dan pengguna modul juga diharapkan bisa mencegah penipuan digital dengan mengkritisi informasi sekaligus bisa berpartisipasi dalam melaporkan penipuan digital jika menjadi korban penipuan digital.

Sementara itu, Kurnia dkk. (2022) menawarkan berbagai solusi praktis bagi pengguna digital, yang ditujukan terutama kepada kaum muda di Indonesia Timur, tak hanya untuk memahami berbagai modus penipuan digital namun juga untuk mencegah dan menangani penipuan digital. Tak hanya itu, konteks hukum penipuan digital pun dikenalkan dalam buku panduan literasi digital tersebut.

METODE RISET

Riset ini merupakan riset nasional pertama di Indonesia yang memetakan modus, medium, dan rekomendasi penipuan digital di Indonesia.

Dilakukan dari Februari hingga Juni 2022, kegiatan riset ini terbagi ke dalam tahapan sebagai berikut.

1. Studi pustaka
2. *Focus Group Discussion* (FGD) pertama mengenai jenis penipuan digital
3. Olah dan analisis data FGD
4. Penyusunan kuesioner survei
5. Uji coba kuesioner survei
6. Analisis data uji coba survei
7. Penyempurnaan kuesioner survei
8. Survei (penyebaran kuesioner pada responden)
9. Olah dan analisis data survei
10. *Focus Group Discussion* kedua dan ketiga mengenai modus, medium, dan rekomendasi penipuan digital dengan responden survei terpilih
11. Olah dan analisis data FGD
12. Penyusunan buku laporan riset

Riset nasional mengenai penipuan digital di Indonesia ini menggunakan pendekatan *mixed-method* yang memadukan pendekatan kuantitatif yang menggunakan metode survei dan kualitatif yang menggunakan FGD.

Metode survei dilakukan secara daring dengan sampling non-probabilitas yang melibatkan 1.700 responden dari kelompok responden yang bervariasi demografinya di 34 provinsi Indonesia. Pemilihan sampel dengan tingkat marjin kesalahan ±2,38% dan tingkat kepercayaan sebesar 95 % ini dapat dilihat persebarannya di tiap provinsi dalam Gambar 1.3.

Gambar 1.3. Sebaran Jumlah Responden Per Provinsi

1700
Total Responden

Total Sampel per wilayah

1595 Umum (usia produktif)

105 Lansia

	Sampel per wilayah	Umum (usia produktif)	Lansia
304 Jawa Barat		286	18
256 Jawa Timur		241	15
230 Jawa Tengah		213	17
93 Sumatera Utara		87	6
75 Banten		70	5
66 DKI Jakarta		62	4
57 Lampung		54	3
57 Sulawesi Selatan		54	3
53 Sumatera Selatan		50	3
40 Riau		38	2
35 Sumatera Barat		33	2
34 Nusa Tenggara Timur		32	2
34 Kalimantan Barat		32	2
33 Aceh		31	2
33 Nusa Tenggara Barat		31	2
27 Bali		25	2
27 Papua		25	2
26 Kalimantan Selatan		24	2
24 Kalimantan Timur		23	1
23 DI Yogyakarta		22	1
22 Jambi		21	1
19 Sulawesi Tengah		18	1
17 Kalimantan Tengah		16	1
17 Sulawesi Tenggara		16	1
16 Sulawesi Utara		15	1
13 Bengkulu		12	1
13 Kep Riau		12	1
12 Maluku		12	0
9 Kep Bangka Belitung		8	1
9 Sulawesi Barat		8	1
8 Maluku Utara		8	0
7 Gorontalo		6	1
7 Papua Barat		7	0
4 Kalimantan Utara		3	1

Sumber: olahan tim peneliti

Jumlah sampel di setiap provinsi mempertimbangkan jumlah penduduk yang ada di masing-masing provinsi. Provinsi dengan jumlah penduduk yang banyak juga diwakili oleh jumlah sampel yang lebih banyak, seperti Jawa Barat, Jawa Tengah, dan Jawa Timur. Dalam pengambilan sampel, tim peneliti juga mem-pertimbangkan keterwakilan penduduk lanjut usia.

Bingkai *sampling* adalah warga Indonesia yang berusia 17 tahun ke atas termasuk warga senior yang di atas usia 60 tahun ke atas. Selain kriteria usia, responden juga harus aktif menggunakan SMS/telepon, aplikasi percakapan, media sosial, maupun platform digital lainnya setidaknya satu tahun terakhir. Riset ini juga mengupayakan keseimbangan gender di antara responden.

Metode survei daring dipilih karena memungkinkan peneliti melakukan pemetaan suatu persoalan, seperti halnya penipuan digital, dengan melibatkan responden berjumlah banyak pada masa pandemi COVID-19. Survei merupakan metode yang tepat ketika peneliti menghendaki mengumpulkan data orisinal untuk mendeskripsikan populasi yang besar dan sulit dijangkau jika melakukan observasi secara langsung (Babbie, 2013).

Survei nasional ini melibatkan 44 enumerator dari 34 provinsi untuk membantu penyebaran kuesioner melalui Google Form yang disebarkan secara terbatas untuk menjaga kualitas sampling sebagaimana yang direncanakan.

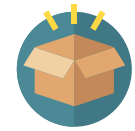
Penggunaan Google Form ini dilakukan untuk mengumpulkan data dari responden. Data kemudian diolah dengan menggunakan SPSS dan Microsoft Excel. Instrumen survei berupa kuesioner yang disusun berdasarkan hasil kajian literatur dan FGD yang melibatkan 11 korban penipuan digital. FGD pertama ini dilakukan untuk mengeksplorasi persoalan penipuan digital yang mungkin belum dijumpai dalam literatur. Tim peneliti berasumsi, mungkin ada yang khas dari penipuan digital ini di Indonesia, dan tidak dibahas dalam literatur yang sebagian besar merupakan tulisan peneliti-peneliti luar negeri.

Berdasarkan tinjauan pustaka, pemberitaan mengenai penipuan digital di Indonesia, dan FGD dengan para korban penipuan digital yang dilakukan sebelum survei, peneliti mengelompokkan penipuan digital menjadi 15 modus yang dilakukan melalui delapan medium atau saluran komunikasi. Lima belas modus penipuan itu adalah:

Gambar 1.4. Modus Penipuan Digital


Penipuan berkedok hadiah


Pengiriman tautan/*link* yang berisi *malware*/virus


Penipuan jual beli


Situs web/ aplikasi palsu


Penipuan berkedok krisis keluarga


Pinjaman *online* ilegal


Penipuan berkedok amal

Investasi ilegal


Lowongan kerja palsu


Pencurian data pribadi


Peretasan dompet digital/rekening bank


Penipuan arisan *online*


Penipuan berkedok asmara


Penerimaan sekolah/ beasiswa palsu


Pemerasan penerimaan kerja

Sumber: olahan tim peneliti

Gambar 1.5. Medium Penipuan Digital

Sumber: olahan tim peneliti

Lima belas modus penipuan dan delapan medium tersebut selanjutkan digunakan peneliti saat menanyakan pengalaman 1.700 responden melalui kuesioner. Kuesioner terdiri dari 39 pertanyaan dengan sub-sub pertanyaan yang ada di dalamnya. Responden mengalokasikan waktu 7-10 menit untuk dapat mengisi kuesioner.

Adapun proses pengumpulan data, secara teknis, dilakukan dengan menghubungi enumerator dan enumerator merekrut responden berdasarkan pada bingkai sampel dan jumlah sampel sudah ditentukan. Enumerator kemudian mendata responden yang bersedia berpartisipasi dalam penelitian dan mengirimkan tautan Google Form yang berisi kuesioner. Tim peneliti melakukan pemantauan setiap hari untuk memastikan kuesioner terisi semua dan tidak ada kesalahan dalam pengisian.

Dengan melibatkan sejumlah besar responden yang mewakili 34 provinsi, survei ini diharapkan bisa menghasilkan data nasional yang merepresentasikan pengalaman warga Indonesia dari beragam kelompok demografi dan geografi dalam mengalami dan menavigasi penipuan digital. Dengan begitu pemetaan terhadap insiden, medium, korban, kerugian, respons, dan rekomendasi bisa dilakukan.

Untuk memperdalam temuan riset secara kuantitatif, riset ini juga menggunakan pendekatan kualitatif dengan melibatkan 20 responden terpilih sebagai peserta dua *Focus Group Discussion* (FGD).

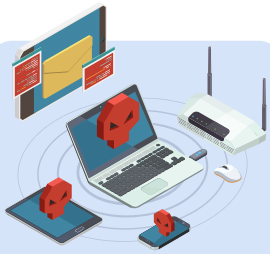
Beberapa pertanyaan yang dielaborasi dalam FGD tersebut antara lain:

Dengan begitu tak hanya pengalaman peserta FGD terkait penipuan digital, tapi juga kerugian, alasan respons, dan usulan rekomendasi mereka ikut memperkaya temuan riset ini.

SISTEMATIKA BUKU

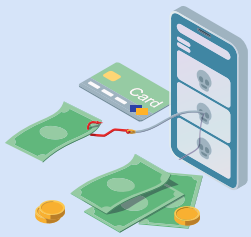
Urgensi Riset Nasional Penipuan Digital di Indonesia

Profil Responden Survei Nasional Penipuan Digital di Indonesia



Pesan dan Medium Penipuan Digital

Korban Penipuan Digital



Kerugian Korban Penipuan Digital

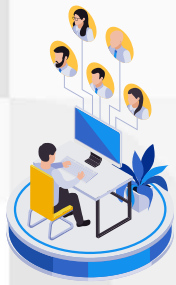
Respon Penipuan Digital

Rekomendasi untuk Mengatasi Penipuan Digital

Penutup

2

PROFIL RESPONDEN DAN INFORMAN



PROFIL RESPONDEN DAN INFORMAN

Bab ini memaparkan profil responden yang berpartisipasi dalam penelitian ini. Profil responden meliputi jenis kelamin, usia, tingkat pendidikan, status pernikahan, jenis pekerjaan, jumlah pendapatan, dan domisili responden.

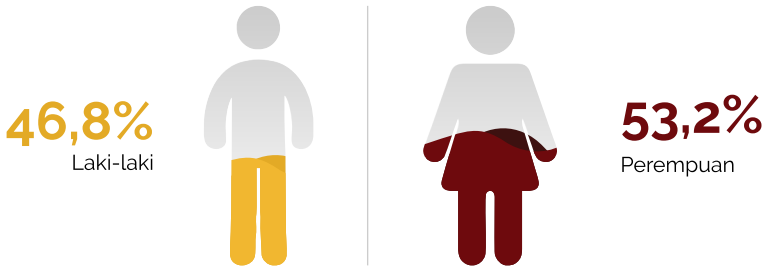
Tak hanya profil demografis yang telah disebutkan, bab ini juga mengulas kebiasan responden dalam menggunakan internet, jumlah waktu yang dihabiskan responden untuk berselancar di internet setiap hari, ragam kegiatan yang membutuhkan paling banyak waktu ketika mengakses internet, serta perbandingan ragam kegiatan daring yang paling menyita waktu antar generasi usia.

Selain memetakan profil responden survei, bab ini juga menjelaskan profil informan yang terlibat dalam serial FGD mengenai penipuan digital yang dilakukan sebelum dan sesudah survei.

JENIS KELAMIN RESPONDEN

Penelitian ini melibatkan 1.700 responden dari 34 provinsi di Indonesia. Sebanyak 53.2% merupakan responden perempuan dan 46.8% responden laki-laki, dengan usia, tingkat pendidikan, jenis pekerjaan, tingkat pendapatan, dan domisili yang beragam.

Gambar 2.1. Jenis Kelamin Responden

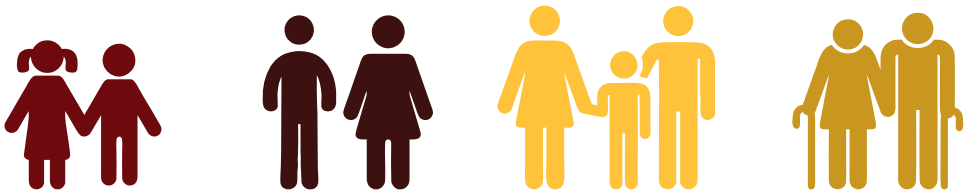


USIA RESPONDEN

Usia responden berkisar antara 18-82 tahun dengan rata-rata usia 32 tahun. Usia responden dikategorikan dalam kelompok generasi usia mengacu pada pengkategorian oleh Badan Pusat Statistik (BPS) dalam Laporan Hasil Sensus Penduduk 2020 (Indonesia. Badan Pusat Statistik, 2020). Generasi *Baby Boomer* (lahir pada tahun 1946-1964), generasi X (lahir pada tahun 1965-1980), generasi Y atau Milenial (lahir pada tahun 1981-1996), dan generasi Z (lahir pada taun 1997-2012).

Untuk menyederhanakan pengkategorian, dalam penelitian ini generasi Pre-Boomer (lahir pada atau sebelum 1945) dimasukkan ke dalam kategori *Baby Boomer* dan generasi Post Z (lahir pada atau setelah 2012) dimasukkan ke dalam kategori generasi Z. Mayoritas responden adalah generasi Z (46,59%), generasi Milenial (30,53%), generasi X (16,24%), dan generasi *Baby Boomer* (6,65%). Proporsi generasi usia responden penelitian yang ditunjukkan oleh Gambar 2.2 selaras dengan proporsi generasi usia penduduk Indonesia menurut Laporan Hasil Sensus Penduduk 2020 BPS, di mana generasi Z merupakan kelompok usia yang jumlahnya paling mendominasi, disusul oleh generasi Milenial, generasi X, dan *Baby Boomer*.

Gambar 2.2. Jumlah Responden Berdasarkan Usia



46,59%
792 - Generasi Z:
1997-2012
(10-25 tahun)

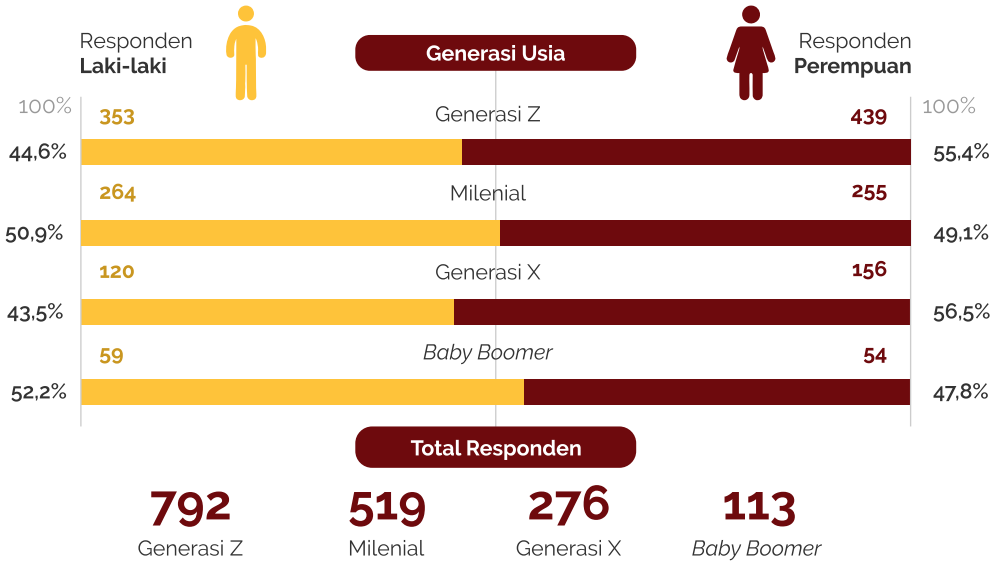
30,53%
519 - Milenial:
1981-1996
(26-41 tahun)

16,24%
276 - Generasi X:
1965-1980
(42-57 tahun)

6,65%
113 - *Baby Boomer*:
1946-1964
(58-76 tahun)

Proporsi responden laki-laki dan perempuan hampir berimbang pada setiap generasi usia, seperti ditunjukkan Gambar 2.3. Pada generasi X dan Z, jumlah responden perempuan lebih mendominasi daripada responden laki-laki (masing-masing 56,5% dan 55,4%). Sebaliknya pada generasi *Baby Boomer* dan Milenial, persentase responden laki-laki sedikit lebih banyak daripada responden perempuan (masing-masing 52,2% dan 50,9%).

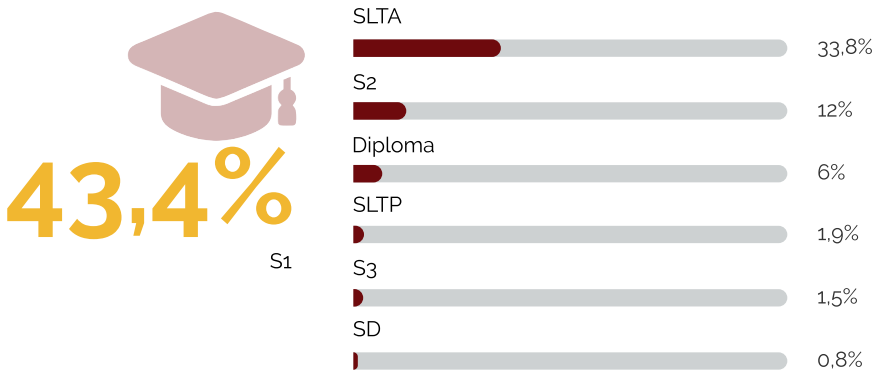
Gambar 2.3. Tabulasi Silang Generasi Usia dan Jenis Kelamin



TINGKAT PENDIDIKAN

Responden dalam penelitian ini memiliki latar belakang tingkat pendidikan yang beragam. Secara komposisi nasional, persentase pendidikan tertinggi yang ditamatkan oleh penduduk Indonesia di atas 15 tahun yang paling besar adalah tingkat SLTA (29,1%) (Indonesia. Badan Pusat Statistik, 2020). Di dalam penelitian ini, mayoritas responden merupakan lulusan S1 (43,41%), disusul lulusan SLTA (33,76%), S2 (12%), Diploma (6,53%), SLTP (1,94%), S3 (1,53%), dan SD (0,82%).

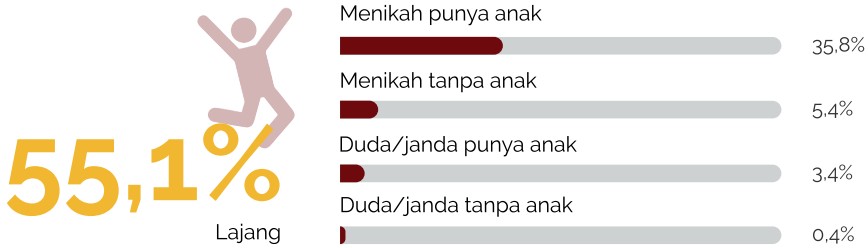
Gambar 2.4. Tingkat Pendidikan Responden



STATUS RESPONDEN

Sebanyak 55,12% responden belum menikah, disusul oleh responden yang menikah dan mempunyai anak (35,82%), responden yang menikah tanpa anak (5,35%), responden yang berstatus duda/janda dan mempunyai anak (3,35%), dan terakhir responden yang berstatus duda/janda tanpa anak (0,4%).

Gambar 2.5. Status Responden



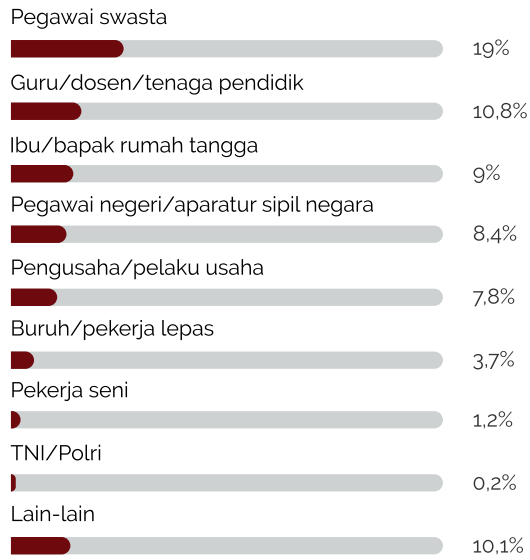
JENIS PEKERJAAN RESPONDEN

Mayoritas responden berprofesi sebagai pelajar dan mahasiswa (29,8%), disusul pegawai swasta (19%), guru/dosen/tenaga pendidik (10,82%), ibu atau bapak rumah tangga (9%), aparatur sipil negara (8,41%), pelaku usaha (7,76%), buruh atau pekerja lepas (3,71%), pekerja seni (1,18%), dan TNI/Polri (0,24%). Responden yang tidak mengindentifikasi dirinya dengan pekerjaan-pekerjaan yang ada dalam pilihan pekerjaan yang telah disebutkan, mengisi pilihan lain-lain (10,1%).

Gambar 2.6. Pekerjaan Utama Responden

29,8%

Mahasiswa/pelajar



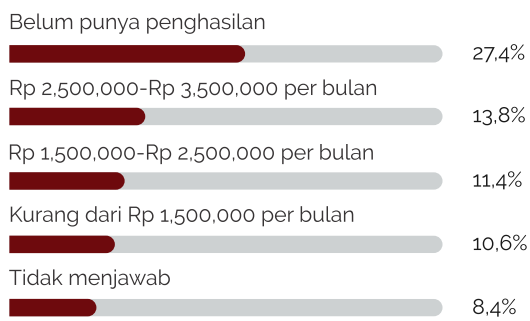
PENDAPATAN RATA-RATA PER BULAN

Sebanyak 28,5% responden mempunyai pendapatan lebih dari Rp3.500.000 per bulan, disusul oleh 27,4% responden yang belum berpenghasilan. Besarnya jumlah responden yang belum berpenghasilan ini kemungkinan terkait dengan jumlah responden pelajar dan mahasiswa yang mencakup hampir 30% dari keseluruhan jumlah responden. Berikutnya, sebanyak 13,76% responden mempunyai kisaran pendapatan Rp2.500.000-Rp3.500.000, 11,41% responden pada kisaran Rp1.500.000-Rp2.500.000, dan 10,65% responden berpendapatan di bawah Rp1.500.000. Sejumlah 8,35% responden memilih untuk tidak menjawab.

Gambar 2.7. Pendapatan Rata-rata Per Bulan Responden

28,5%

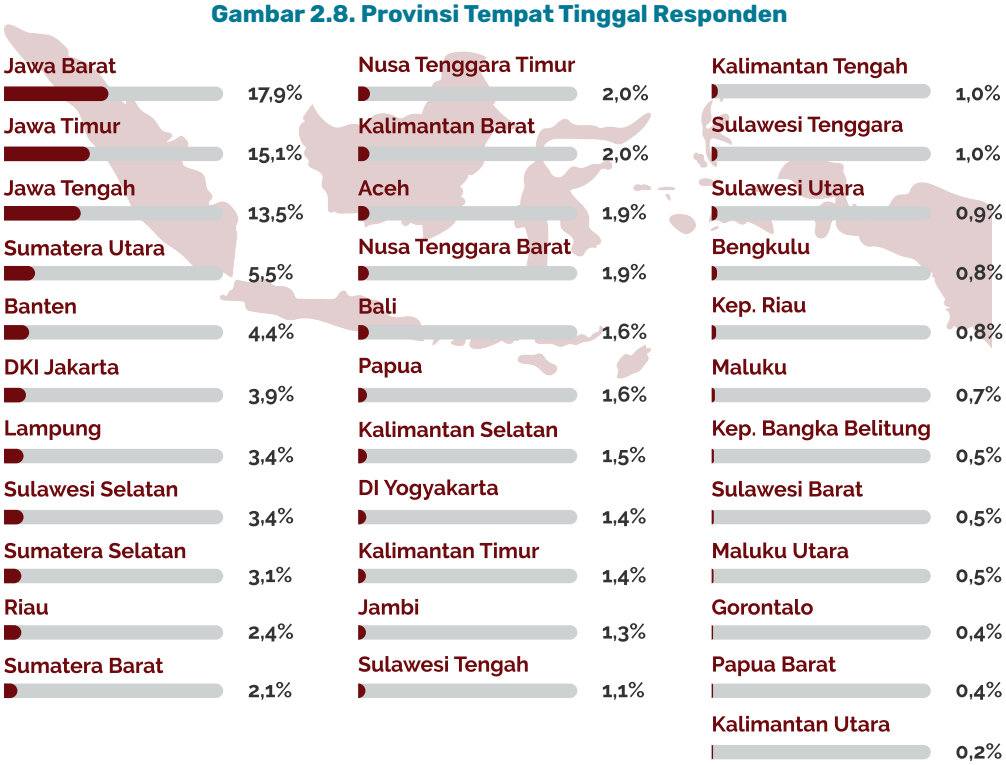
Lebih dari
Rp. 3.500.000 per bulan



PROVINSI TEMPAT TINGGAL

Jumlah responden pada tiap provinsi beragam, proposinya disesuaikan dengan distribusi jumlah penduduk atau populasi total pada masing-masing provinsi. Lima besar provinsi dengan jumlah responden terbanyak antara lain, Jawa Barat (17,9%), Jawa Timur (15,1%), Jawa Tengah (13,5%), Sumatera Utara (5,5%), dan Banten (4,4%). Provinsi dengan jumlah responden paling sedikit yaitu Kalimantan Utara, sebesar 0,2% dari total 1.700 responden penelitian.

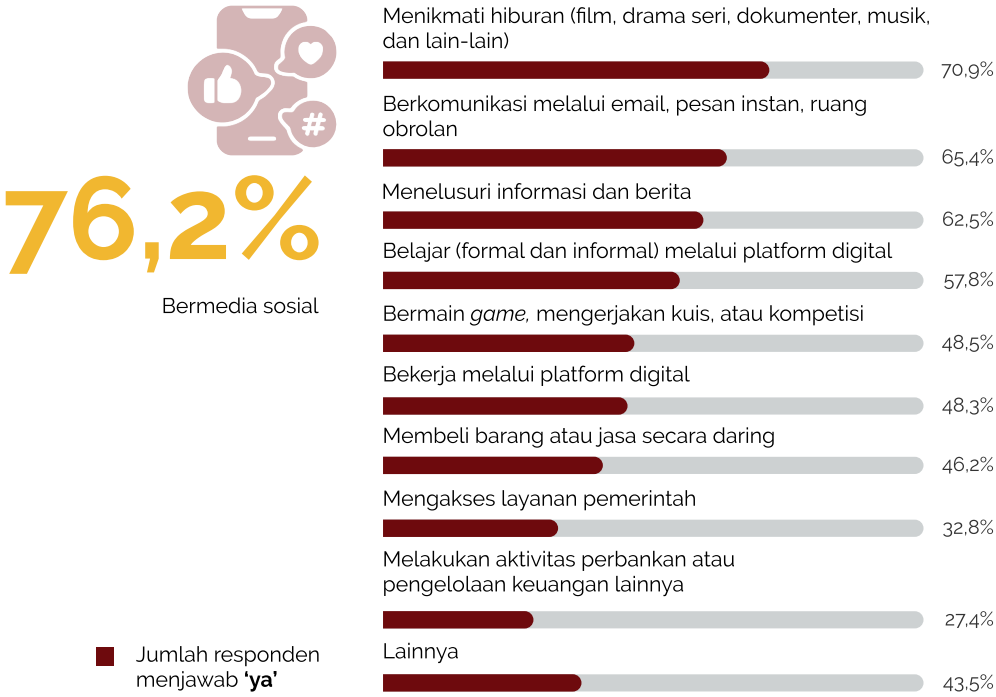
Gambar 2.8. Provinsi Tempat Tinggal Responden



RAGAM KEGIATAN DARING

Rata-rata waktu per hari yang dihabiskan responden dalam berkegiatan daring beragam, berkisar antara kurang dari setengah jam hingga hampir 24 jam terkoneksi dan melakukan kegiatan daring. Gambar 2.9 menunjukkan ragam kegiatan yang paling menyita waktu responden. Setiap responden harus memberikan jawaban 'Ya' atau 'Tidak' pada masing-masing jenis kegiatan, sehingga persentase yang muncul pada setiap jenis kegiatan adalah persentase dari total jumlah responden, yaitu 1.700.

Gambar 2.9. Kegiatan Daring yang Paling Menyita Waktu



Dari sepuluh jenis kegiatan, empat kegiatan yang paling banyak mendapatkan jawaban 'Ya' dari responden adalah kegiatan bermedia sosial (76,2%), menikmati hiburan (film, drama seri, dokumenter, musik, dan lain-lain) (70,9%), berkomunikasi secara daring (melalui email, pesan instan, maupun ruang obrolan) (65,4%), dan menelusuri informasi dan berita (62,5%). Masa pandemi yang mengondisikan masyarakat untuk bekerja maupun belajar dari rumah membuat pilihan jenis kegiatan belajar (baik secara formal maupun informal) melalui platform digital serta bekerja melalui platform digital disepakati responden sebagai aktivitas yang paling banyak menyita waktu responden, masing-masing oleh sebanyak 57,8% dan 48,3% responden. Jenis kegiatan daring yang paling sedikit dianggap responden sebagai kegiatan yang paling menyita waktu yaitu kegiatan mengakses layanan pemerintah (32,8%) dan kegiatan perbankan atau pengelolaan keuangan lainnya (27,4%).

Sebanyak 43,5% responden menjawab kegiatan-kegiatan lain yang belum termasuk ke dalam kategori kegiatan pilihan jawaban yang tersedia.

Kegiatan-kegiatan tersebut diantaranya, menjual barang dan jasa, persiapan melamar pekerjaan (mencari informasi lowongan maupun mengikuti kursus persiapan), mencari referensi (misalnya, untuk keperluan belajar mengajar serta mengamati reviu sebelum membeli barang atau jasa), serta mengikuti kegiatan keagamaan (ibadah/kajian/ceramah).

Temuan ini serupa dengan data We Are Social & Kepios (2022), yang mengungkap bahwa rata-rata waktu paling tinggi yang dihabiskan penduduk Indonesia pengguna internet berusia 16-64 tahun ketika berselancar di internet adalah untuk berkegiatan di media sosial (3 jam 17 menit). Rata-rata ini lebih tinggi daripada rata-rata waktu menonton televisi atau musik secara *streaming* (masing-masing 2 jam 50 menit dan 1 jam 40 menit) atau membaca berita (1 jam 40 menit). Sumber yang sama menyebutkan bahwa tiga urutan teratas motivasi pengguna internet berusia 16-64 tahun dalam mengakses internet adalah untuk mengakses informasi (80,1%), mendapatkan ide dan inspirasi (72,9%), dan berkomunikasi dengan keluarga dan teman (68,2%).

Persamaan dan perbedaan kebiasaan melakukan kegiatan daring yang paling memakan banyak waktu antar generasi usia dapat dilihat pada Gambar 2.10. Persentase pada tabel merupakan persentase dari total jumlah responden pada masing-masing generasi usia, generasi Z sebanyak 792 responden, generasi Milenial sebanyak 519 responden, generasi X sebanyak 276 responden, dan *Baby Boomer* sebanyak 113 responden.

Pada generasi Z, beberapa kegiatan yang disepakati paling menyita banyak waktu adalah bermedia sosial (80,2%), menikmati hiburan (76,6%), berkomunikasi daring (66,8%), belajar (62,2%), dan juga bermain game (59,1%). Menurut riset GWI, generasi Z merupakan generasi yang paling merasa menghabiskan terlalu banyak waktu di media sosial dibandingkan dengan 3 generasi sebelumnya (GWI, 2022).

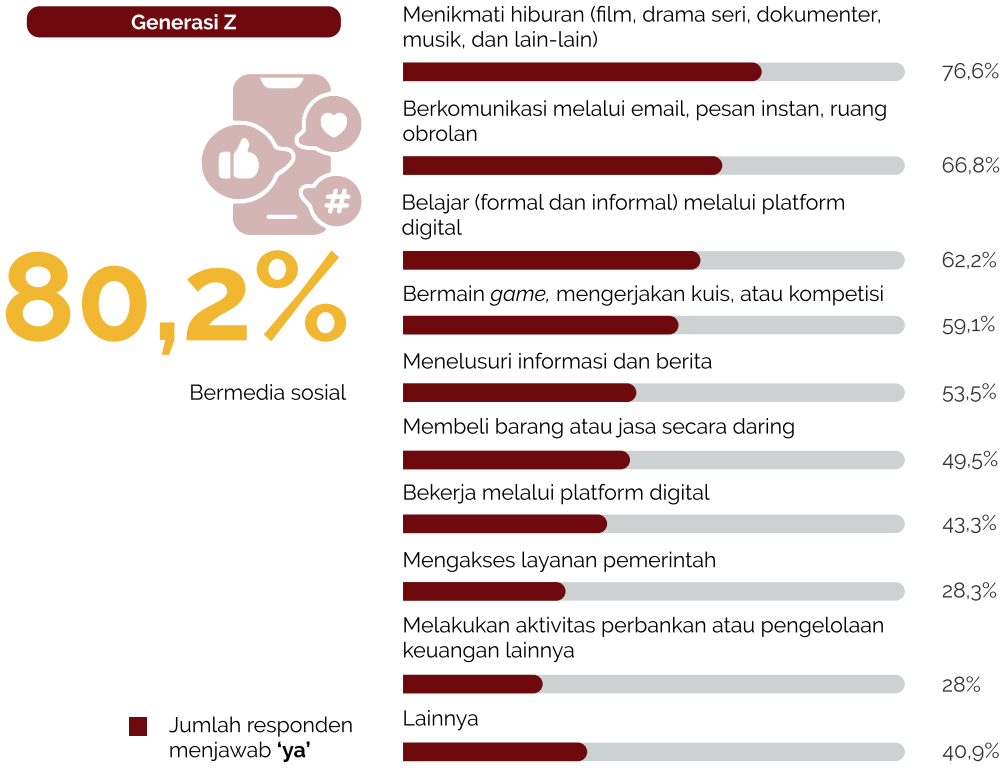
Tren yang hampir yang sama juga terlihat pada generasi Milenial, di mana aktivitas bermedia sosial dianggap oleh mayoritas responden sebagai kegiatan daring yang paling menyita waktu (77,1%), disusul kegiatan menikmati hiburan (71,9%), berkomunikasi daring (65,5%), dan belajar (60,3%).

Yang membedakan dengan generasi Z, pada generasi Milenial kegiatan menelusuri informasi dan berita menduduki peringkat ketiga kegiatan yang paling banyak membutuhkan alokasi waktu (69,6%).

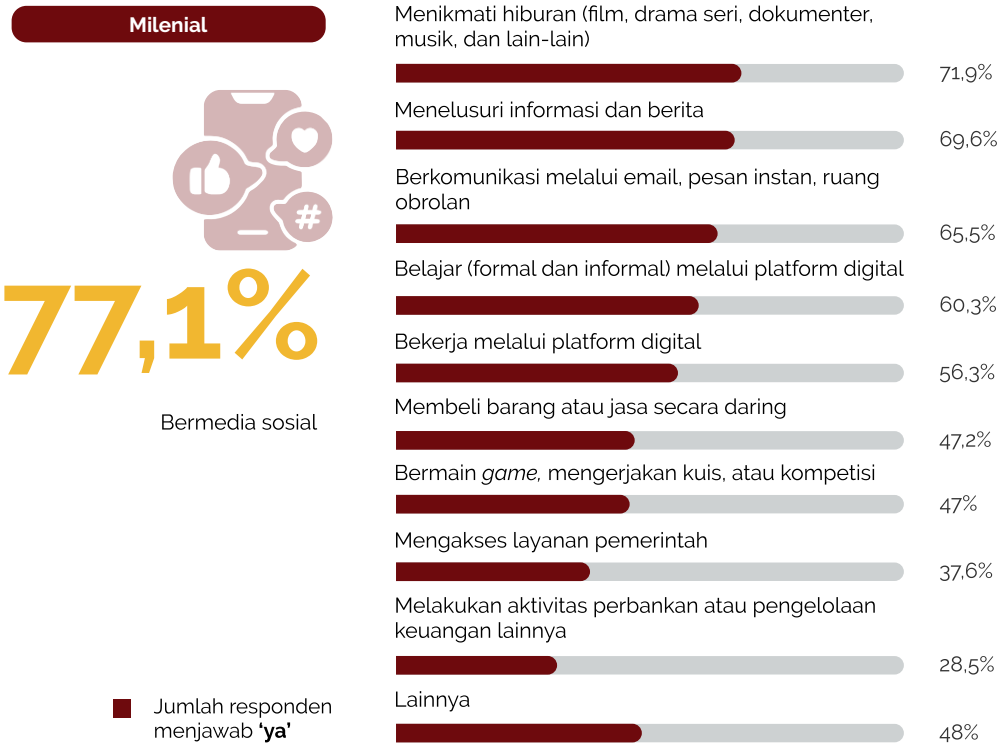
Pada generasi X, kegiatan menelusuri informasi dan berita berada pada peringkat pertama (72,5%), disusul oleh bermedia sosial (70,3%), berkomunikasi secara daring (65,2%), menikmati hiburan (58,7%), dan bekerja melalui platform digital (57,6%).

Kegiatan menelusuri berita juga menjadi kegiatan yang paling banyak mendapatkan afirmasi dari generasi *Baby Boomer* sebagai kegiatan yang paling banyak menyita waktu (69%). Beberapa kegiatan lain yang persentasenya cukup besar dalam generasi ini antara lain, bermedia sosial (58,4%), berkomunikasi secara daring (55,8%), menikmati hiburan (55,8%), serta membeli barang atau jasa secara daring (33,6%).

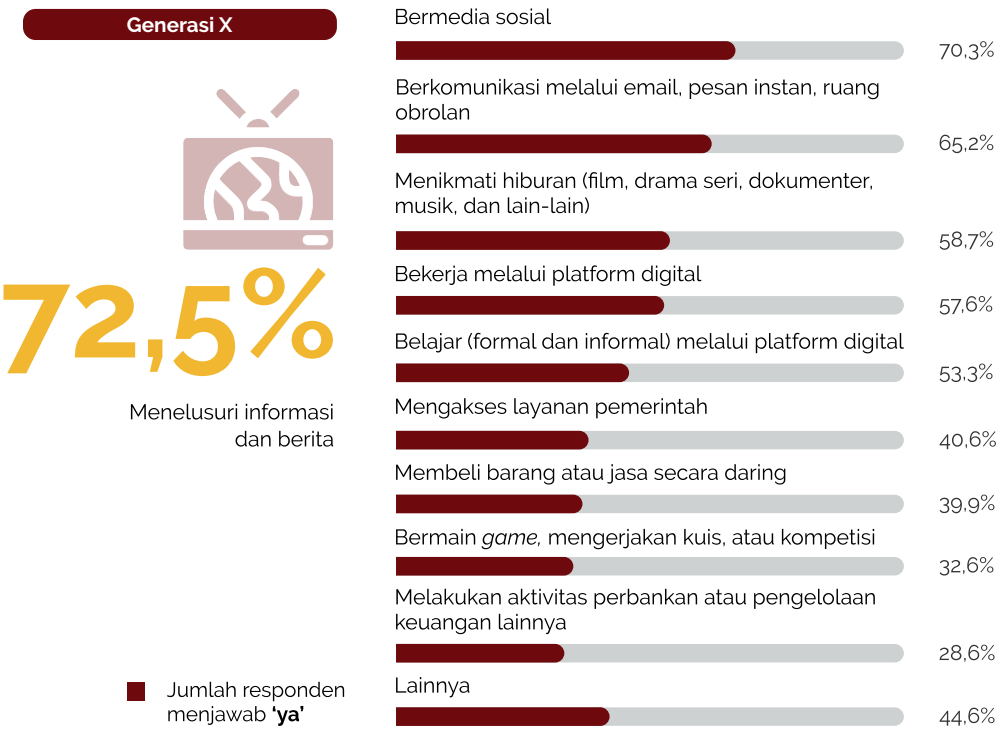
Gambar 2.10.1. Kegiatan Daring yang Paling Menyita Waktu antar Generasi Usia



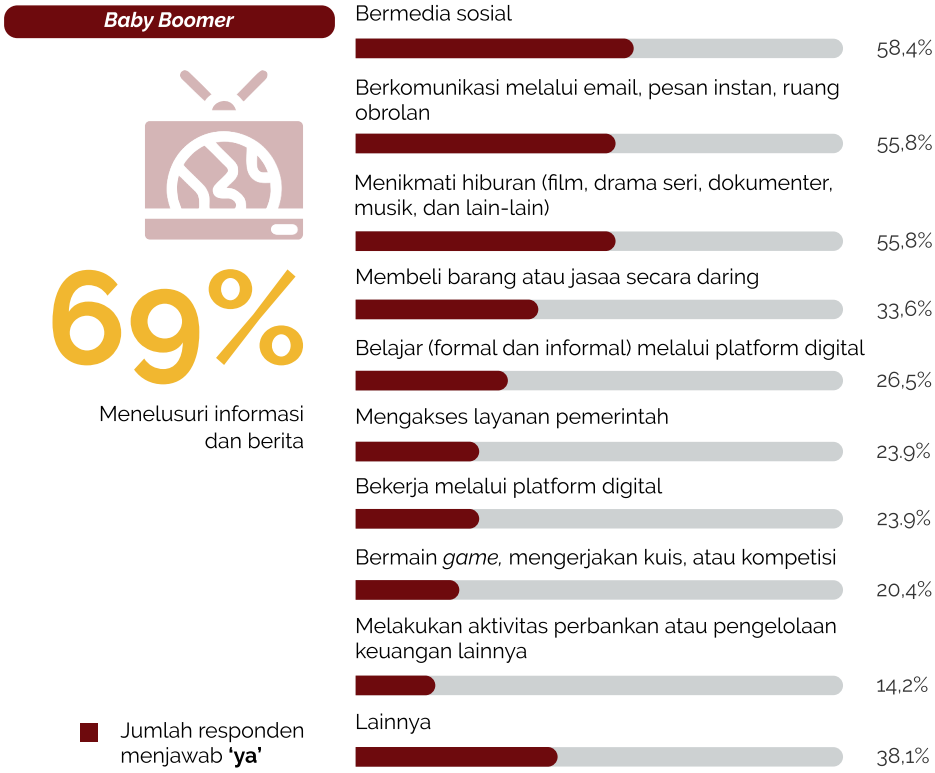
Gambar 2.10.2. Kegiatan Daring yang Paling Menyita Waktu antar Generasi Usia



Gambar 2.10.3. Kegiatan Daring yang Paling Menyita Waktu antar Generasi Usia



Gambar 2.10.4. Kegiatan Daring yang Paling Menyita Waktu antar Generasi Usia



Melalui ulasan bab ini diketahui bahwa mayoritas responden riset ini termasuk ke dalam kelompok usia generasi Z (lahir pada atau setelah tahun 1997). Jumlah responden laki-laki dan perempuan cukup berimbang, meskipun proporsi responden perempuan sedikit lebih banyak. Pendidikan terakhir responden didominasi oleh S1 dan SLTA. Relevan dengan riset-riset yang pernah dilakukan mengenai kebiasaan berinternet penduduk Indonesia, kegiatan bermedia sosial menempati peringkat atas kegiatan daring yang paling menyita waktu responden (peringkat pertama pada generasi Z dan Milenial, peringkat kedua pada generasi X dan *Baby Boomer*). Selain itu kegiatan mencari informasi atau berita dan juga kegiatan mencari hiburan juga mendapatkan peringkat yang cukup tinggi antar kelompok usia.

Bab ini diharapkan dapat memberikan konteks bagi bab-bab selanjutnya yang akan mengaitkan temuan-temuan penelitian dengan karakteristik demografis maupun kebiasaan responden dalam berkegiatan daring.

PROFIL PESERTA *FOCUS GROUP DISCUSSION* (FGD)

FGD pada penelitian ini diadakan dalam dua tahap. FGD pertama yang diselenggarakan pada 12 Februari 2022 bertujuan untuk mencatat dan memetakan pengalaman pengguna internet di Indonesia yang pernah menjadi korban penipuan digital, untuk selanjutnya bersama hasil kajian pustaka digunakan sebagai bahan untuk menyusun kuesioner survei. FGD kedua diselenggarakan pada 9 April 2022. FGD ini bertujuan untuk memperdalam data yang didapatkan dari survei, dengan menggali situasi dan kondisi yang dialami korban. Temuan FGD kedua menjadi dasar penyusunan rekomendasi yang menyeluruh untuk pencegahan dan penanganan penipuan digital yang berorientasi kepada kebutuhan dan ekspektasi korban. Profil peserta FGD pertama (awal) dan kedua (akhir) akan dijelaskan dalam dua bagian.

Profil Peserta FGD Awal

FGD awal melibatkan informan yang pernah menjadi korban penipuan digital. Peserta dipilih melalui *convenience sampling*, dengan asas kemudahan akses oleh peneliti kepada informan yang memenuhi kriteria penelitian. Kriteria peserta FGD awal adalah berkewarganegaraan Indonesia dan pernah menjadi korban penipuan digital. Untuk mendapatkan gambaran awal yang menyeluruh mengenai kejadian penipuan digital, keragaman penipuan digital yang dialami, keseimbangan gender, dan variasi usia menjadi pertimbangan dalam memilih peserta FGD.

Dari 12 orang yang diundang, 11 orang hadir dalam FGD, dengan proporsi 5 orang perempuan dan 6 laki-laki. Usia peserta FGD berkisar dari 19 hingga 52 tahun, dengan latar belakang domisili, tingkat pendidikan, dan pekerjaan yang beragam. Kasus penipuan yang dialami responden pun beragam, dari penipuan berkedok hadiah melalui SMS atau telepon dan aplikasi *chat,* jual beli fiktif, hingga saldo di akun *e-wallet* yang berkurang sendiri tanpa dipakai transaksi oleh pemilik akun.

Hal-hal yang digali dari peserta FGD antara lain pengalaman menjadi korban penipuan digital, tindakan yang dilakukan setelah mengalami penipuan (melaporkan atau tidak melaporkan), dampak yang dialami, dan rekomendasi terhadap otoritas untuk mencegah dan menangani penipuan digital.

FGD ini menghasilkan identifikasi awal jenis penipuan digital, modus operandi, dampak yang dialami, hingga rekomendasi dari peserta untuk pemangku kepentingan.

Profil Peserta FGD Akhir

FGD akhir melibatkan informan yang sebelumnya menjadi responden survei dalam penelitian ini. Teknik pemilihan sampel menggunakan *purposive sampling* dengan kriteria berkewargenegaraan Indonesia, menjadi responden dalam survei penipuan digital, pernah menjadi korban penipuan, aktif menggunakan media sosial/aplikasi *chat*/SMS/telepon, serta berusia minimal 18 tahun.

Pemilihan peserta FGD juga mendasarkan pada keragaman jenis penipuan yang dialami korban, medium yang digunakan penipu untuk menghubungi korban, serta dampak yang dirasakan korban. Selain itu, latar belakang demografis (gender, domisili, generasi usia, tingkat pendidikan) juga menjadi pertimbangan untuk menghadirkan variasi situasi dan pengalaman dalam FGD.

Sebanyak 24 informan diundang untuk hadir di dalam FGD. Informan dihubungi melalui nomor kontak yang dicantumkan pada saat mengisi kuesioner. Agar diskusi berjalan dengan intensif, forum FGD dibagi menjadi dua forum dan diselenggarakan secara paralel. FGD dibagi menjadi dua forum dengan mempertimbangkan intensitas diskusi. FGD A dilakukan dengan peserta yang merupakan responden terpilih dari wilayah waktu Indonesia Tengah dan Indonesia Timur. Sedangkan FGD B dilakukan dengan peserta dari wilayah waktu Indonesia Barat. Jumlah peserta FGD B atau informan yang berdomisili di Indonesia Barat lebih banyak daripada peserta yang berdomisili di masing-masing Indonesia Tengah dan Indonesia Timur karena pertimbangan proporsi jumlah dalam populasi.

Pada FGD A, dari 12 calon peserta yang diundang, 10 orang hadir dalam FGD, terdiri atas 6 laki-laki dan 4 perempuan. Informan berdomisili di Sulawesi Selatan, Sulawesi Tenggara, Sulawesi Barat, Maluku Utara, Nusa Tenggara Barat, Nusa Tenggara Timur, Bali, dan Papua. Usia informan berkisar dari 23 hingga 58 tahun. Latar belakang pendidikan informan meliputi SMA, Diploma, Sarjana, dan Magister.

Sama halnya dengan FGD A, untuk FGD B dari 12 orang yang diundang, 10 orang memenuhi undangan FGD. Peserta FGD B terdiri atas 8 perempuan dan 2 laki-laki dengan kisaran usia 18 hingga 60 tahun. Informan berdomisili di Jawa Barat, Jawa Timur, DI Yogyakarta, dan Lampung. Salah satu peserta berasal dari provinsi Sulawesi Selatan yang seharusnya menjadi bagian dari peserta FGD Indonesia Tengah. Tingkat pendidikan informan bervariasi, dari SMA, Diploma, Sarjana hingga Magister.

FGD akhir berusaha mendalami modus yang dilakukan pelaku penipuan dan faktor-faktor yang membuat korban terjebak dalam penipuan dan atau faktor-faktor yang membuat informan terhindar dari jebakan penipuan digital. Selain itu informan juga diminta untuk mengungkapkan perasaan yang dirasakan saat mengalami atau nyaris mengalami penipuan. Sama seperti pada FGD awal, informan juga diberikan pertanyaan mengenai tindakan yang dilakukan saat mengalami penipuan, apakah melaporkan atau tidak melaporkan tindak penipuan kepada pihak berwenang. Sebagai penutup, informan diminta untuk memberikan rekomendasi pencegahan dan penanganan kasus penipuan digital di Indonesia.

3

PESAN DAN MEDIUM PENIPUAN DIGITAL

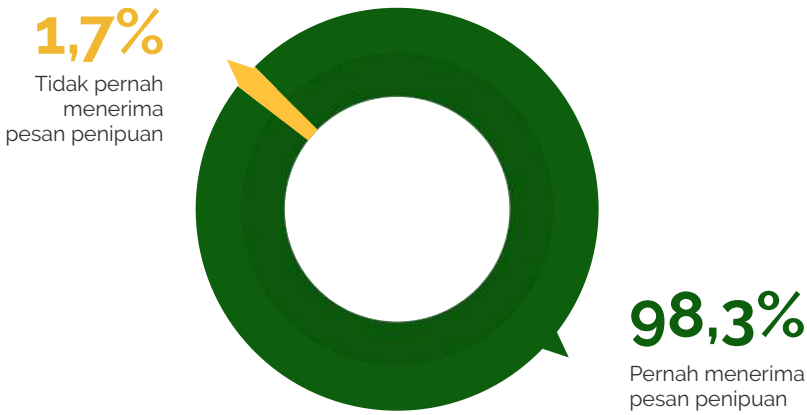
PESAN DAN MEDIUM PENIPUAN DIGITAL

Dari 15 jenis penipuan digital yang diulas dalam penelitian ini, bab ini akan menguraikan pesan penipuan apa yang paling sering diterima responden hingga yang paling jarang. Selanjutnya, bab ini juga mengulas melalui medium apa responden menerima pesan-pesan penipuan tersebut.

PESAN PENIPUAN DIGITAL

Dari 1.700 responden yang berpartisipasi, sebanyak 98,3% (1.671 responden) pernah menerima pesan penipuan digital. Hal ini menunjukkan rentannya warga Indonesia dalam menerima berbagai pesan penipuan digital di keseharian mereka.

Gambar 3.1. Persentase Responden yang Pernah Menerima Pesan Penipuan (N=1.700)



Jenis Penipuan Digital yang Diterima

Responden dapat memilih lebih dari satu jenis isi pesan penipuan yang pernah dialami sehingga persentase pada setiap jenis penipuan adalah persentase dari total jumlah responden (1.700).

Lima jenis penipuan yang paling banyak diterima responden adalah penipuan berkedok hadiah (91,2%), pinjaman digital ilegal (74,8%), pengiriman tautan yang berisi *malware* atau virus (65,2%), penipuan berkedok krisis keluarga (59,8%), dan investasi ilegal (56%). Sedangkan lima jenis penipuan yang paling sedikit diterima respoden diantaranya penerimaan sekolah/beasiswa palsu (19,9%), penerimaan pada proses penerimaan kerja (20,6%), pembajakan/peretasan akun dompet digital (25,6%), penipuan berkedok asmara/romansa (27, 7%), dan pencurian identitas pribadi (29,2%).

Gambar 3.2. Jenis Penipuan Digital yang Diterima

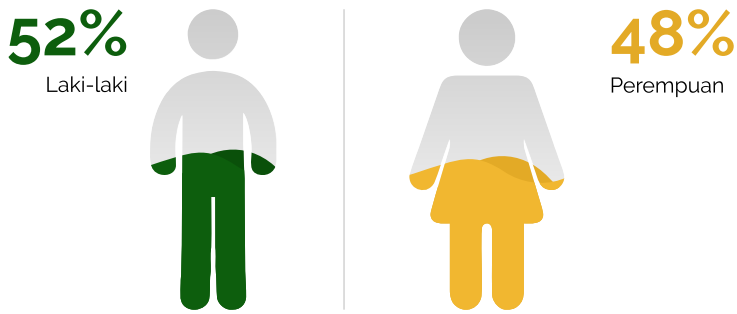
Penipuan berkedok hadiah menjadi jenis pesan penipuan yang paling sering diterima responden karena sifatnya yang cenderung disampaikan secara random dan massal melalui berbagai jenis medium, terutama melalui fitur yang melekat pada setiap telepon seluler (panggilan atau SMS).

Frekuensi pesan penipuan pinjaman dan investasi ilegal yang terbilang tinggi di dalam penelitian ini selaras dengan temuan Satgas Waspada Investasi (SWI) bahwa selama pandemi, pengaduan pinjaman digital ilegal mengalami peningkatan yang sangat signifikan (Burhan, 2021), demikian halnya dengan kasus investasi ilegal (Sulaiman, 2021). Menurunnya kemampuan ekonomi masyarakat akibat pembatasan darurat selama pandemi dan kemudahan syarat pinjaman ditengarai menjadi penyebab maraknya penipuan berkedok pinjaman digital dalam masa pandemi.

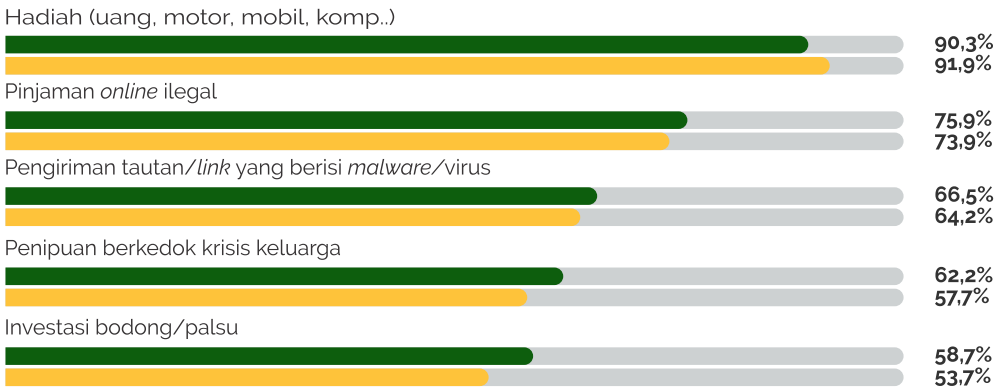
Jenis Penipuan Digital yang Diterima Berdasarkan Gender

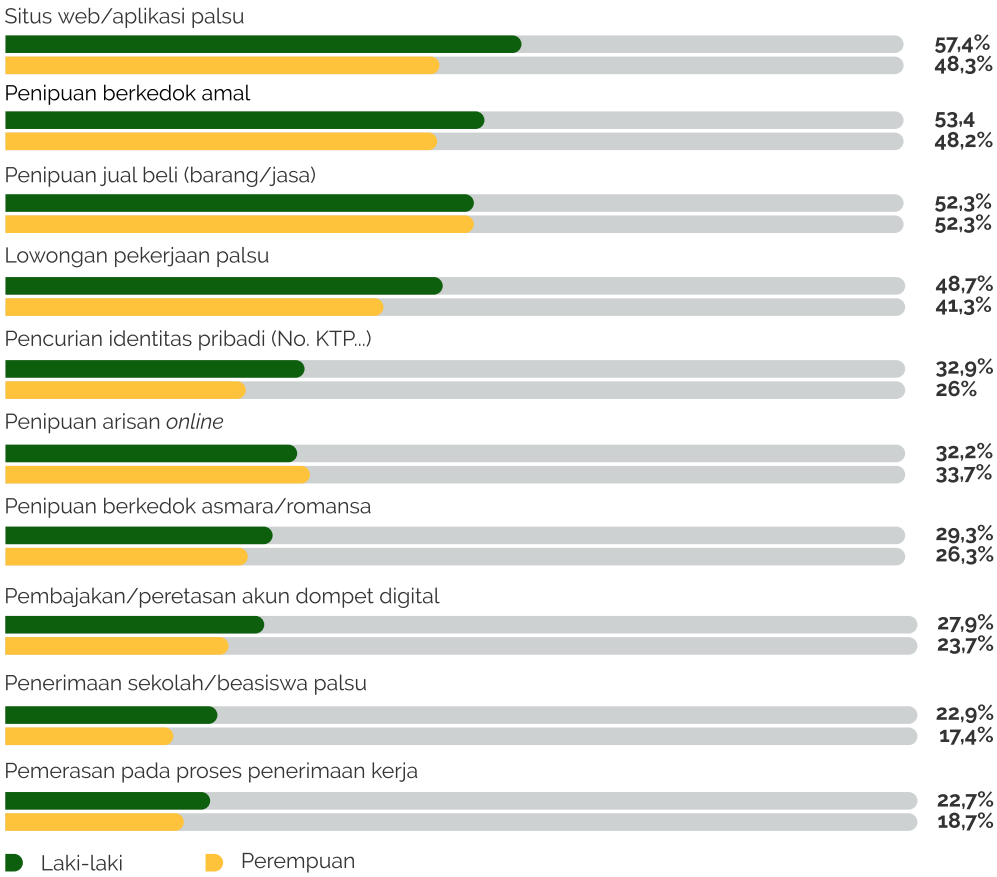
Secara total, persentase responden laki-laki yang pernah menerima pesan penipuan lebih banyak (52%) daripada responden perempuan (48%) untuk keseluruhan jenis pesan penipuan, seperti ditunjukkan oleh Gambar 3.3. Persentase penerimaan pesan berdasarkan gender untuk setiap jenis penipuan dapat dilihat pada Gambar 3.4.

Gambar 3.3. Pesan Penipuan yang Diterima Berdasarkan Gender (N=1700)



Gambar 3.4. Persentase Jenis Pesan Penipuan yang Diterima berdasarkan Gender





Ragam Pengalaman Penerimaan Pesan Penipuan

Di bawah ini adalah cerita-cerita yang disampaikan oleh para informan di dalam FGD tentang pengalaman mereka menerima pesan penipuan digital. Kisah pertama adalah seseorang yang menjadi korban penipuan berkedok hadiah (lewat SMS atau panggilan telepon), jenis pesan yang paling banyak diterima oleh responden survei.

> *"HP bunyi sampai tujuh kali, terus karena sudah geregetan, saya angkat dan katanya saya menang undian cashback dari suatu lokapasar senilai dua juta lima ratus ribu."* **(EA, 25 tahun, FGD, 12 Februari 2022)**

Pesan penipuan juga dapat berkaitan dengan identitas pribadi penerima pesan. Pengiriman pesan jenis ini sering kali memanfaatkan situasi psikologis korban, misalnya pada pesan penipuan berkedok krisis keluarga sebagai berikut.

"...dia telepon ketika saya baru saja sampai kantor, katanya istri saya kecelakaan. Padahal sebelum saya ke kantor, saya mengantar istri ke bandara...Hah kecelakaan? Saya langsung waswas kan..." **(AA, 44 tahun, FGD, 12 Februari 2022)**

Penyalahgunaan identitas seseorang atau sebuah lembaga juga ditemukan pada penipuan jual beli, di mana pelaku mengirim pesan penipuan dengan mengatasnamakan penjual yang kredibel, sehingga audiens cenderung mempercayai pesan yang disampaikan. Selain itu jumlah pengikut media sosial atau lokapasar yang banyak juga mendorong calon korban untuk mempercayai pesan penipuan jual beli.

"...sebelumnya saya lihat...itu ada tokonya, toko fisiknya itu ada di sebuah jalan di Condet itu saya lihat, oh ini bener nih." **(Mu, 49 tahun, FGD, 12 Februari 2022)**

"Followers-nya itu kebetulan waktu itu ada tiga ribu lebih atau seribu lebih gitu, saya lupa. Pokoknya dia itu sebelumnya udah trusted, gitu." **(JH, 19 tahun, FGD, 12 Februari 2022)**

Meskipun jenis penipuan beragam, beberapa informan sepakat bahwa penipu mampu menyampaikan pesan secara meyakinkan, misalnya dengan menggunakan identitas perusahaan yang resmi di dalam pesan sehingga membuat korban percaya bahkan sampai mau melakukan instruksi yang diminta oleh pelaku.

"Tapi, sama sekali saya tidak curiga...Karena, ya itu, logonya X, formulirnya X, sampai nomor operator...pun punya X." **(ED, 43 tahun, FGD, 9 April 2022)**

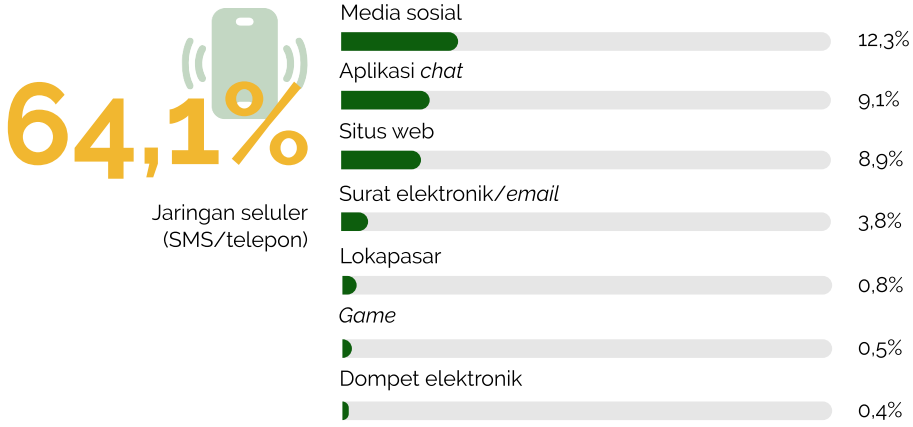
Pada beberapa kasus, pesan disampaikan dengan cara memanipulasi perasaan korban, yang berujung pada pemerasan.

"Di media sosial saling kenal, saling dekat, terus tukaran nomor kontak,...katanya dia mau mencairkan uang senilai 200 juta...lalu dia pinjam uang dari tante saya senilai 30 juta." **(IL, 28 tahun, FGD, 9 April 2022)**

MEDIUM PENIPUAN DIGITAL

Dari delapan medium yang disediakan, jaringan seluler (SMS/telepon) merupakan medium yang paling banyak dipakai pelaku penipuan, yang urutannya tampak dalam tabel di bawah ini.

Gambar 3.5. Delapan Medium yang Digunakan Penipu untuk Mengirim Pesan Penipuan



Jaringan seluler (SMS/telepon) ini terutama dipakai untuk mengirim pesan penipuan berkedok hadiah, yang kebanyakan dikirimkan melalui SMS. Sebagai catatan, penipuan berkedok hadiah merupakan modus yang paling banyak diterima responden sekaligus paling banyak memakan korban di antara responden. Mengirim pesan penipuan melalui SMS memang berbiaya murah, jangkauannya paling luas dibanding medium lain, dan sangat mudah karena merupakan fitur sangat sederhana pada ponsel.

Di bawah ini adalah gambar yang menunjukkan pesan atau modus penipuan dan medium yang paling sering digunakan untuk mengirimkannya.

Gambar 3.6. Pesan/Modus Penipuan dan Medium yang Paling Sering Digunakan

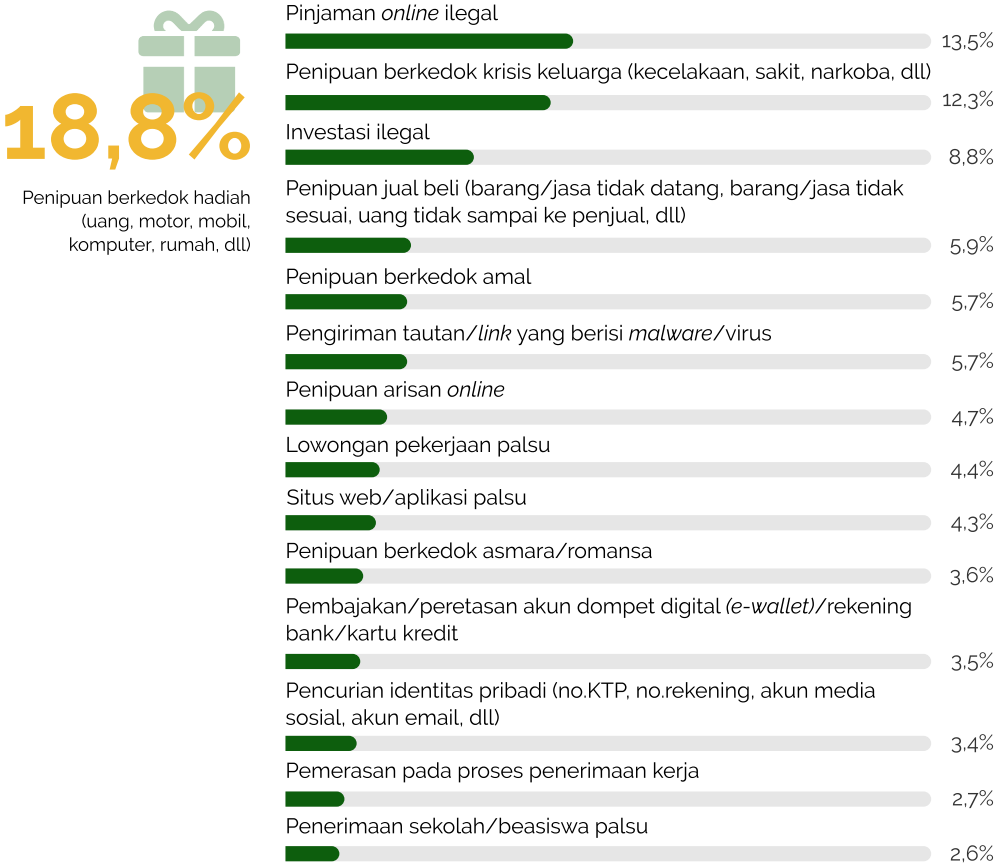
	Modus	Medium
1	Penipuan berkedok hadiah	Jaringan seluler (SMS/Telepon)
2	Penipuan berkedok krisis keluarga	Jaringan seluler (SMS/Telepon)
3	Penipuan jual beli	Jaringan seluler (SMS/Telepon)
4	Peretasan akun dompet digital/ rekening bank	Dompet Elektronik
5	Pencurian data pribadi	Dompet Elektronik
6	Investasi ilegal	Jaringan seluler (SMS/Telepon)
7	Pinjaman *online* ilegal	Jaringan seluler (SMS/Telepon)
8	Lowongan kerja palsu	Surat elektronik
9	Pemerasan penerimaan kerja	Surat elektronik
10	Penerimaan sekolah/beasiswa palsu	Surat elektronik
11	Pengiriman tautan berisi*malware*/ virus	Situs web
12	Penipuan berkedok asmara	Aplikasi *chat*
13	Situs web/aplikasi palsu	Situs web
14	Penipuan arisan *online*	Media sosial
15	Penipuan berkedok amal	Aplikasi *chat*

Selanjutnya adalah uraian temuan survei dari delapan medium dan 15 pesan atau modus penipuan yang menyertainya, dari yang paling sering ke paling jarang.

Jaringan Seluler (SMS/Telepon)

Dari delapan medium, sebagian besar pesan penipuan (total 15 modus penipuan) dikirimkan penipu melalui medium seluler, terutama melalui SMS. Ini bisa dikatakan terkait dengan pengiriman SMS yang sangat mudah, murah, dan bisa menjangkau paling banyak calon korban dibanding tujuh medium lainnya.

Gambar 3.7. Urutan Modus Operandi yang Dilakukan Melalui Jaringan Seluler (SMS/Telepon)



FGD yang dilakukan bersama para korban menunjukkan, kasus penipuan berkedok hadiah terutama dilakukan melalui SMS yang diikuti dengan panggilan telepon.

"Saya mendapat SMS, lalu saya ditelepon bahwa saya menang hadiah. Saat itu seperti terhipnotis, diarahkan ke ATM, dan dipesan supaya jangan sampai putus koneksi, instruksinya sangat rapat. Tapi ternyata saldo ATM saya kosong lalu diminta pinjam ke teman. Saya pun pinjam 100 ribu ke teman kantor bagian keuangan. Saya dipantau dan dipandu terus, lalu saya transfer pulsa 100 ribu ke penipu. Saat diminta transfer lagi, saya baru sadar bahwa ini penipuan. Setelah itu saya masih sering menerima SMS bahwa saya menang hadiah dari banyak nomor." **(DE, 44 tahun, FGD, 9 April 2022)**

Permasalahan lain dengan nomor seluler juga diuraikan oleh DE sebagai berikut.

"Saya baru saja beli nomor seluler baru, langsung masuk banyak SMS dan (panggilan) telepon tagihan yang ditujukan ke pemilik nomor lama. Padahal saya beli nomor itu di counter secara resmi, dan melakukan registrasi sesuai ketentuan Kominfo. Sebaiknya operator tidak menjual kembali nomor seluler yang sudah tidak aktif karena bisa jadi pemilik lama itu bermasalah."

Sementara itu, penipuan berkedok krisis keluarga terutama dilakukan melalui panggilan telepon. Salah satu upaya penipuan dialami oleh seorang informan FGD, yang bercerita:

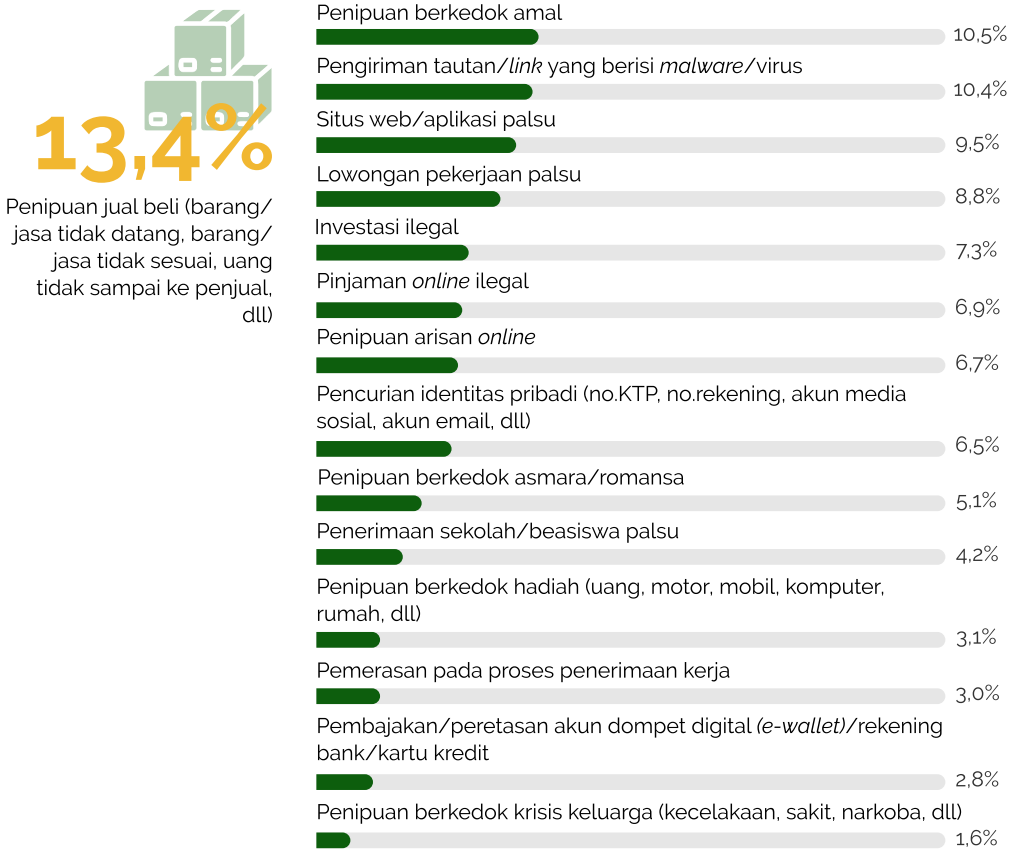
"Saya dihubungi orang tua di kampung bahwa mereka menerima telepon di rumah (landline), bahwa kakak saya kecelakaan, masuk rumah sakit. Orang tua diminta kirim 20 juta, jika tidak kirim maka kakak saya tidak ditangani. Sebelumnya, kakak saya ditelepon orang yang mengaku polisi, bahwa kakak saya terlibat narkoba. Sehingga kakak saya mematikan ponselnya, karena tidak mau diteror. Karena tidak bisa menghubungi kakak, saya menelepon teman kakak saya untuk memastikan, ternyata kakak saya ada di kos, baik-baik saja." **(LD, 29 tahun, FGD, 9 April 2022)**

Media Sosial

Medium terbanyak kedua adalah media sosial, yang mencakup platform digital seperti YouTube, Facebook, Instagram, Twitter, TikTok, dan lain-lain. Mayoritas pesan atau modus penipuan yang dikirim melalui media sosial adalah jual-beli barang dan jasa dengan sebagian besar pelaku penipuan adalah penjual, meski kadang ada pembeli juga yang menipu, seperti mengirimkan bukti transfer palsu dan penjual tidak melakukan pengecekan secara baik.

Jadi dalam jenis penipuan jual-beli, barang atau jasa yang ditransaksikan bisa tidak datang ke pembeli, tidak sesuai dengan yang dijanjikan di media sosial, dan uang tidak sampai ke penjual.

Gambar 3.8. Urutan Modus Operandi yang Dilakukan Melalui Media Sosial



Salah satu korban penipuan jual-beli yang dilakukan melalui media sosial dialami oleh AF, yang menceritakan pengalamannya dalam FGD:

> *"Saya membeli sandal di akun Instagram, yang followers dan testimoninya banyak. Sehingga saya percaya saja. Setelah saya transfer 500 ribu, saya diminta transfer lagi 50 ribu karena ini jasa titip. Setelah berhari-hari, barang tak kunjung tiba."* **(AF, 18 tahun, FGD, 9 April 2022)**

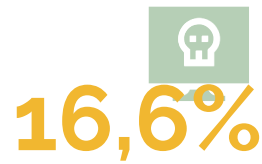
Pengalaman lain diceritakan oleh DE, yang melibatkan pengiriman pesan melalui Instagram dan WhatsApp.

"Ada akun IG berjualan sepeda, muncul melalui sponsored content, dan menawarkan giveaway atau hadiah sepeda juga. Jika mau mendapatkan silakan DM. Saya pun kirim DM, lalu diminta pindah ke WA, dan diminta transfer ongkir 250 ribu. Setelah itu ya si penipu menghilang, sepeda tidak datang. Banyak sekali penipuan jual beli di IG. Followers, testimoni, dan komen yang banyak itu tidak menjamin." **(DE, 44 tahun, FGD, 9 April 2022)**

Aplikasi *Chat*

Jenis penipuan yang paling banyak dilakukan melalui aplikasi *chat* adalah pengiriman tautan/*link* yang berisi *malware*/virus, yang bisa digunakan oleh pelaku kejahatan untuk melakukan *phishing* atau mengumpulkan data pribadi korban. Selain itu, responden juga menyatakan bahwa penipuan berkedok amal atau bantuan sosial juga sering mereka terima melalui aplikasi *chat,* yang mencakup antara lain platform WhatsApp, Telegram, dan LINE.

Gambar 3.9. Urutan Modus Operandi yang Dilakukan Melalui Aplikasi *Chat*



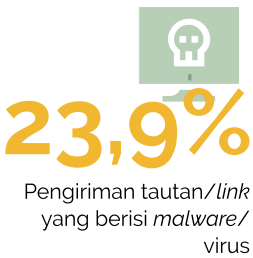
Di dalam FGD bersama para korban penipuan digital, salah satu peserta menceritakan pengalamannya menerima teror melalui WhatsApp dari penyedia pinjaman *online,* yang ia tidak tahu apakah itu pinjol legal atau ilegal.

> *"Teman saya berutang ke pinjol, dan menurut orang pinjol itu, saya dijadikan jaminan. Kalau teman saya tidak membayar, saya akan diteror terus. Teman saya tidak bisa saya hubungi, jadi terpaksa saya block nomor pinjol itu, karena pesan dan teleponnya sungguh mengganggu."* **(LD, 29 tahun, FGD, 9 April 2022)**

Situs Web

Penipuan ini terjadi saat korban sedang mengakses situs web apa pun, seperti laman berita dan toko. Lalu di laman tersebut korban mengeklik tautan yang berisi *malware*/virus maupun situs web palsu, yang bisa mencakup informasi pekerjaan palsu, jual-beli palsu, hingga pemerasan. Jadi pengiriman tautan/*link* yang berisi *malware*/virus biasanya berkaitan dengan keberadaan situs web/aplikasi palsu.

Gambar 3.10. Urutan Modus Operandi yang Dilakukan Melalui Situs Web



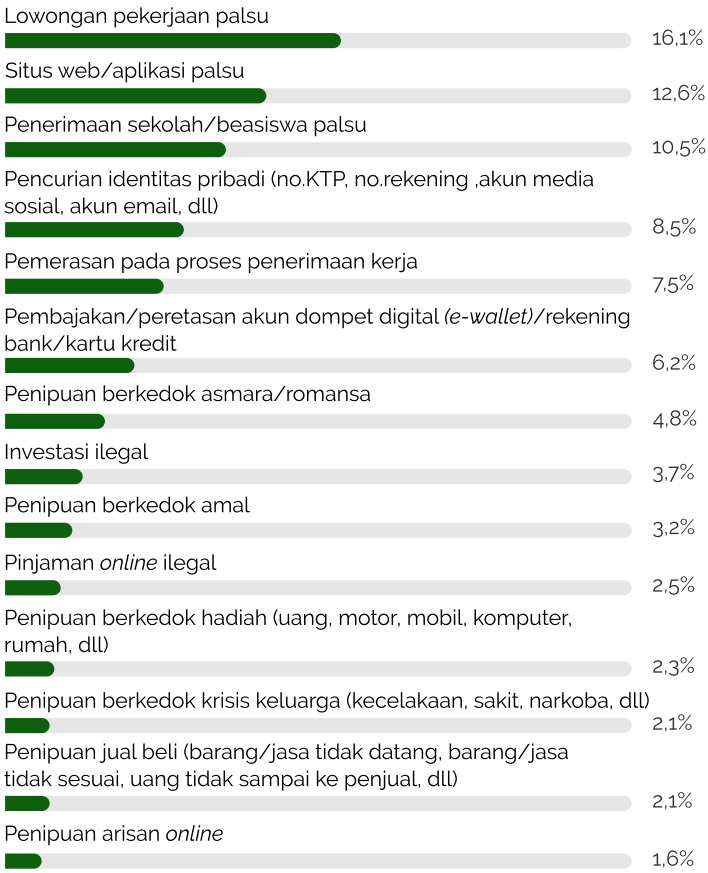
Email

Meski banyak layanan email gratis seperti Google Mail dan Yahoo Mail sudah menyediakan fasilitas untuk menyaring *spam,* email masih menjadi salah satu medium dalam pengiriman pesan penipuan digital. Dua modus penipuan yang paling sering diterima responden melalui email adalah tautan/*link* yang berisi *malware*/virus dan lowongan pekerjaan palsu, yang selengkapnya bisa dilihat di tabel berikut ini.

Gambar 3.11. Urutan Modus Operandi yang Dilakukan Melalui Email

16,5%

Pengiriman tautan/*link* yang berisi *malware*/ virus



Salah satu korban penipuan melalui email terkait lowongan pekerjaan palsu adalah SF, yang menceritakan kisahnya sebagai berikut:

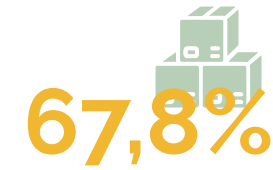
> *"Saya dapat email untuk wawancara pekerjaan dari orang yang mengaku dari sebuah perusahaan besar. Saya ikuti semua prosedurnya, persyaratannya saya kirim. Lalu saya disuruh berangkat ke Jakarta. Supaya bisa cepat, saya diminta menggunakan pesawat terbang dan harus menggunakan agen travel yang mereka tentukan. Jadi saya harus membeli tiket di situ. Setelah saya transfer, tiketnya tidak pernah dikirim ke saya. Lalu saya hubungi nomor telepon yang diberikan lewat email, tapi ternyata sudah tidak aktif."* **(SF, 27 tahun, FGD, 9 April 2022)**

Lokapasar

Lokapasar sudah menerapkan berbagai cara untuk mencegah penipuan jual-beli di platformnya, seperti pemblokiran dan pemberian kredibilitas yang buruk dari pembeli bagi toko yang menjual barang yang kenyataannya berbeda dengan yang ditawarkan. Hal ini membuat kasus penipuan di lokapasar sangat sedikit, hanya 0,8% dari seluruh kasus penipuan yang dialami responden survei.

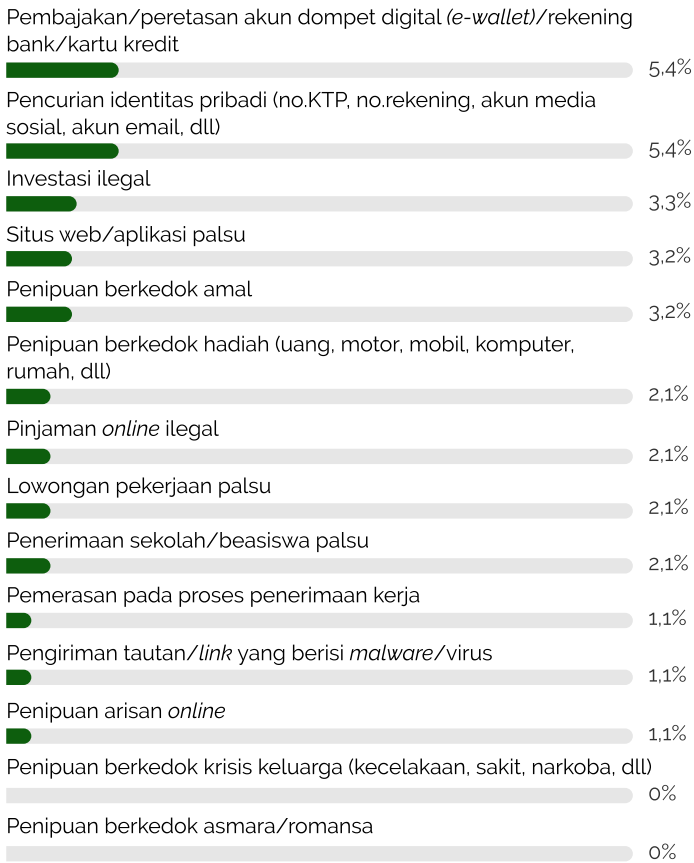
Modus penipuan paling dominan di platform ini berupa penipuan jual-beli, yang diikuti dua modus yang terkait erat dengan isu perlindungan data pribadi, yaitu pembajakan/peretasan akun dompet digital (*e-wallet*)/rekening bank/kartu kredit dan pencurian identitas pribadi (nomor KTP, nomor rekening, akun media sosial, akun email, dll).

Gambar 3.12. Urutan Modus Operandi yang Dilakukan Melalui Lokapasar



67,8%

Penipuan jual beli (barang/jasa tidak datang, barang/jasa tidak sesuai, uang tidak sampai ke penjual, dll)



Lokapasar merupakan salah satu medium digital yang penggunanya meningkat pesat selama pandemi.

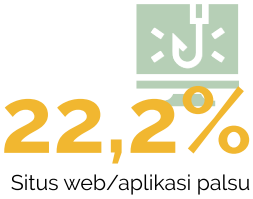
Data global menunjukkan, Indonesia menempati posisi ketiga sebagai negara dengan pengguna aplikasi lokapasar di ponsel Android terbesar di dunia. Jumlah ini meningkat 70% pada periode Januari 2020 hingga Juli 2021 (Riyanto, 2021).

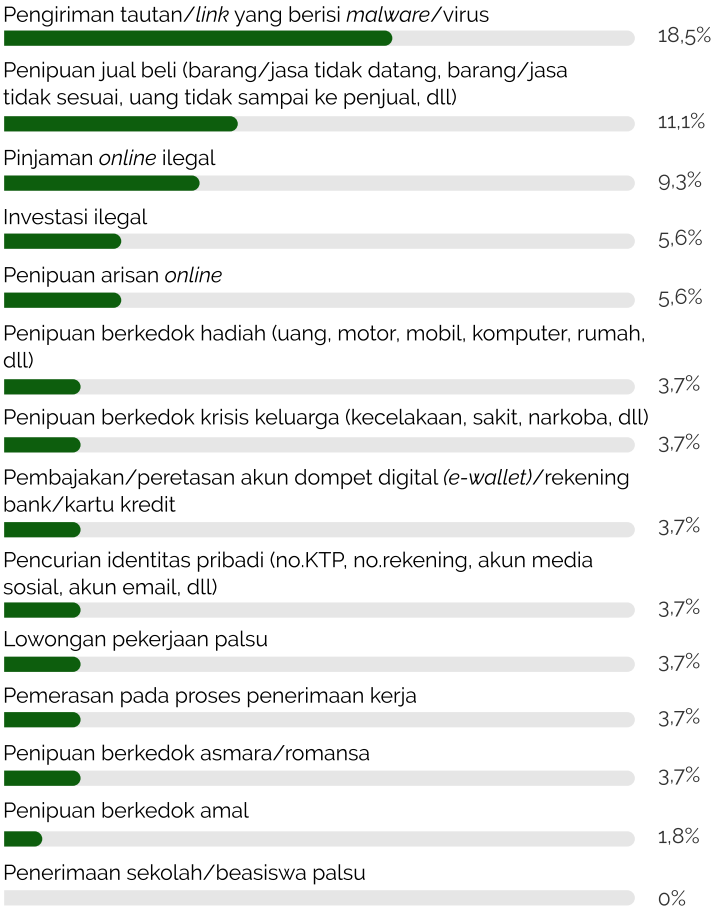
Meski jumlah penipuan digital di lokapasar sangat sedikit dibanding medium lainnya, melihat tren peningkatan penggunanya, langkah pencegahan perlu terus dilakukan oleh platform lokapasar maupun dari sisi konsumen.

Game

Untuk penipuan yang dilakukan melalui situs web atau aplikasi game (0,5 dari total pesan penipuan yang diterima responden), modus terbanyak yang dilakukan melaluinya adalah situs web/aplikasi palsu, yang terkait erat dengan modus terbanyak setelahnya yaitu pengiriman tautan/*link* yang berisi *malware*/virus. Situs web palsu dan pengiriman *malware*/virus ini biasanya dilakukan penipu untuk melakukan *phishing* atau mengumpulkan data pribadi korban yang bermuara pada tindak kriminalitas lain seperti pengambilalihan akun (bank, media sosial, dompet elektronik) milik korban.

Gambar 3.13. Urutan Modus Operandi yang Dilakukan Melalui *Game*





Game online adalah sebuah industri yang secara global bernilai triliunan dolar AS, dengan jenisnya sangat beragam mulai dari permainan kasino di laman hingga aplikasi di ponsel, termasuk *e-sport.* Dengan banyaknya perputaran uang di sana, yang meningkat selama pandemi (King et al., 2020), penipu pun melakukan berbagai aksi untuk mengambil untung dari para pemain.

Hal yang biasa terjadi melalui penipuan pembayaran, mengingat *game* perlu dilakukan dengan pembelian koin atau "mata uang" lain dan ada banyak tawaran di dalamnya untuk kemudahan pemain. Penipuan pembayaran itu biasanya dilakukan dengan menawarkan koin atau upaya untuk mengambil alih kartu kredit pemain (Kount, n.d.).

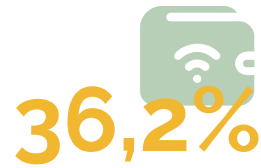
Meski demikian, *game* adalah sebuah area kegiatan daring yang kurang banyak diteliti di Indonesia, terutama dalam kaitannya dengan penipuan.

Oleh karena itu, berdasar data yang sudah ada misalnya tentang jenis-jenis *game* yang populer yang di Indonesia (Aninsi, 2021) dan jumlah penggunanya yang terus meningkat, perlu ada upaya khusus untuk meneliti penipuan digital di jagat *game.*

Dompet Elektronik *(e-wallet)*

Survei ini menunjukkan, dompet elektronik merupakan medium digital yang paling aman dari penipuan digital dibandingkan medium lainnya, yakni hanya 0,4% modus penipuan yang dilakukan melalui dompet elektronik. Ini bisa disebabkan oleh berlapisnya fitur keamanan yang dilakukan oleh platform dompet elektronik untuk memastikan operasional akun sungguh dilakukan oleh pemilik akun yang bersangkutan, seperti pengiriman *one time password* (OTP) ke email, aplikasi *chat,* atau nomor telepon seluler pemilik akun.

Gambar 3.14. Urutan Modus Operandi yang Dilakukan Melalui Dompet Elektronik



36,2%

Pembajakan/peretasan akun dompet digital *(e-wallet)*/rekening bank/ kartu kredit

Meski menempati posisi sebagai medium yang paling aman, aksi kejahatan masih terjadi terhadap pengguna dompet elektronik, terutama dalam bentuk peretasan dan pencurian data pribadi. Salah satu kasusnya dialami oleh AP, yang menceritakan pengalamannya dalam FGD.

> *"Saldo e-wallet saya berkurang karena dipakai orang lain untuk memesan makanan, yang terjadi dua kali, masing-masing sebesar sekitar Rp150 ribu. Setelah kejadian pertama, saya melaporkan kasus pencurian itu ke pegawai e-wallet, kebetulan saya kenal humasnya. Lalu kerugian itu diganti. Namun, kemudian, hal seperti itu terjadi lagi, dan menurut transaksinya, uang itu dipakai untuk membeli makanan yang alamat penerimanya sama dengan kejadian pertama. Saya melaporkan kasus kedua ini ke e-wallet, tapi kali ini tidak ada balasan dan tidak ada penggantian kerugian. Teman saya juga sudah tidak bekerja di sana."* **(AP, 42 tahun, FGD, 12 Februari 2022).**

Kasus peretasan akun dompet elektronik ini unik dan sangat jarang terungkap dalam literatur maupun pemberitaan media.

4

KORBAN PENIPUAN DIGITAL

KORBAN PENIPUAN DIGITAL

Bab ini mengulas korban penipuan digital yang dideskripsikan dari penggabungan temuan dan analisis data kuantitatif (hasil survei daring) dan data kualitatif (hasil FGD daring). Sistematika penjelasannya dimulai dari bagian yang menyajikan presentasi responden survei yang pernah dan tidak pernah menjadi korban, termasuk perjalanan umum sehingga bisa terjebak sebagai korban yang dipelajari dari kisah para peserta dan responden survei yang disampaikan dalam FGD.

Bagian berikutnya adalah deskripsi temuan dari modus penipuan digital berikut korban yang dijeratnya. Ini diikuti analisis silang terhadap korban penipuan digital dan kategori usia, jumlah pendapatan, dan tingkat pendidikan. Harapannya, bab ini dapat memberikan ulasan lengkap terhadap kondisi korban penipuan digital yang ditemukan riset ini.

KORBAN DAN PROSES MENJADI KORBAN PENIPUAN DIGITAL

Gambar 4.1. Korban Penipuan Digital

Dari total 1.700 responden survei, sebanyak 1.132 responden (66,6%) mengaku pernah menjadi korban penipuan digital. Sedangkan 568 responden (33,4%) menyatakan tidak pernah menjadi korban. Perbedaan jumlah yang cukup signifikan ini mengindikasikan bahwa mayoritas responden yang menerima pesan penipuan digital juga terjerat sebagai korban.

Ry (22 tahun), salah satu peserta dalam FGD (12 Februari 2022) yang dilakukan sebelum survei untuk mengetahui cara mengatasi penipuan digital dari perspektif informan yang hampir dan pernah menjadi korban, mengaku mendapatkan SMS yang diikuti dengan telepon selang beberapa menit setelahnya. Sementara itu, AR (24 tahun) dalam FGD yang sama (12 Februari 2022) mengaku justru langsung ditelepon oleh si penipu.

Responden LD (29 tahun, FGD, 9 April 2022) asal Lampung berkata bahwa orang tua dan kakak kandungnya pada waktu yang bersamaan menjadi target dari penipu melalui telepon. Sedangkan IY (35 tahun, FGD, 9 April 2022), responden survei asal Sulawesi Barat bercerita bahwa penipuan digital yang diterima olehnya dan rekannya sama-sama bermula dari SMS dari nomor yang tidak mereka kenal.

FGD juga mengungkap proses yang umum dialami oleh peserta dan responden survei hingga menjadi korban penipuan digital. Sejumlah faktor menjadi penyebabnya, antara lain kondisi psikologis yang diciptakan penipu salah satunya melalui terciptanya rasa yakin semu tentang kedekatan personal, desakan kebutuhan atau solusi yang mendesak, tergiur dengan macam-macam modus seperti iming-iming hadiah, jaminan barang atau jasa yang lebih bagus tapi harganya lebih murah, iklan di media sosial yang dianggap sebagai iklan terpercaya, tertipu penggunaan identitas palsu atau menyerupai aslinya termasuk mencatut identitas nama atau lembaga tertentu, serta rasa empati yang tergerak membantu dalam kasus penipuan berkedok amal atau bantuan sosial.

Salah satu ilustrasi manipulasi psikis ini ditemukan pula dalam literatur terkait penipuan berkedok asmara yang juga terjadi di Indonesia. James Daniel Sinaga adalah salah satu pelaku yang menipu hingga puluhan juta rupiah dengan modus ini melalui aplikasi kencan *online* (Inez, 2022). Korban yang kerap terjerat biasanya merasa kesepian (Retnowati, 2015) tanpa pasangan dan terbuai oleh cerita dan perhatian yang didramatisasi oleh penipu (Rahayu, 2022). Tak sedikit pula, korban terpancing implusif sehingga dengan mudahnya memenuhi permintaan penipu (Whitty, 2017). Bahkan, tak jarang pada penipuan digital umum, penipu memainkan rasa takut dan khawatir dari calon korbannya dengan berbagai cara (Wardani, 2022).

Contoh lain disampaikan oleh responden survei asal Maluku Utara berinisial KJ (38 tahun, 9 April 2022) yang mengatakan bahwa penipu benar-benar cerdas memanfaatkan situasi psikis calon korbannya.

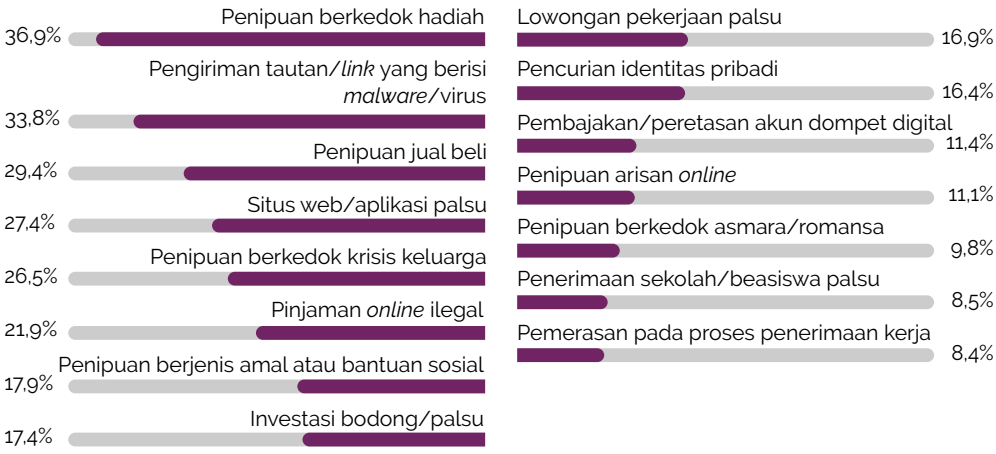
> *"Saya tiba-tiba dapat pesan di aplikasi chat diikuti dengan telepon yang yang mengatasnamakan perusahaan tertentu, dan anehnya mereka seolah tahu kondisi yang tepat untuk melakukan aksi penipuan mereka."*

Sama halnya dengan AY (23, FGD, 9 April 2022), responden asal Nusa Tenggara Barat yang mengaku tergoda secara kejiwaan karena mendengar iming-iming nominal yang fantastis.

> *"Mungkin karena kita mendengar angkanya gede ini dan mungkin secara tidak sadar saya melakukan transaksi."*

Dimensi psikologis ini menjadi pendorong yang tentu saja tidak dapat disamaratakan karena kondisinya bisa berbeda-beda dan dipengaruhi oleh faktor-faktor lainnya. Akan tetapi, kondisi ini nyatanya bisa menjadi faktor intrinsik yang pertama kali menggerakkan para calon korban untuk menindaklanjuti tahapan-tahapan berikutnya sehingga menelan mereka ke dalam pusaran pihak yang merugi.

Gambar 4.2. Modus Penipuan Digital dan Korbannya



MODUS PENIPUAN DIGITAL DAN KORBANNYA

Dari 15 jenis modus penipuan digital yang ditanyakan dalam survei ini, penipuan digital yang paling banyak menjerat korban ialah penipuan berkedok hadiah dengan persentase sebesar 36,9%. Jenis penipuan digital ini diikuti dengan pengiriman tautan berisi *malware*/virus (33,8%), penipuan jual beli (29,4%), situs web/aplikasi palsu (27,4%), dan penipuan berkedok krisis keluarga (26,5%).

Dari lima besar modus penipuan digital tersebut, tiga jenis penipuan digital yakni penipuan berkedok hadiah, pengiriman tautan berisi *malware*/virus, dan situs web/aplikasi palsu tergolong sebagai *mass-marketing fraud/scam*. Modus jenis ini biasanya dikirimkan ke (calon) korban secara massal dan masif serta tidak melibatkan pemalsuan dan pencurian data pribadi (calon) korbannya.

EA (25 tahun, FGD, 12 Feb 2022) mengemukakan bahwa penipuan berkedok hadiah pernah menghampirinya. Setelah penipu meneleponnya berkali-kali, ia akhirnya mengangkatnya dengan informasi dari penipu bahwa dirinya mendapatkan undian *cashback* dari suatu lokapasar senilai jutaan rupiah.

> *"HP bunyi sampe tujuh kali, terus karena sudah geregetan, saya angkat dan katanya saya menang undian cashback dari suatu lokapasar senilai dua juta lima ratus ribu."*

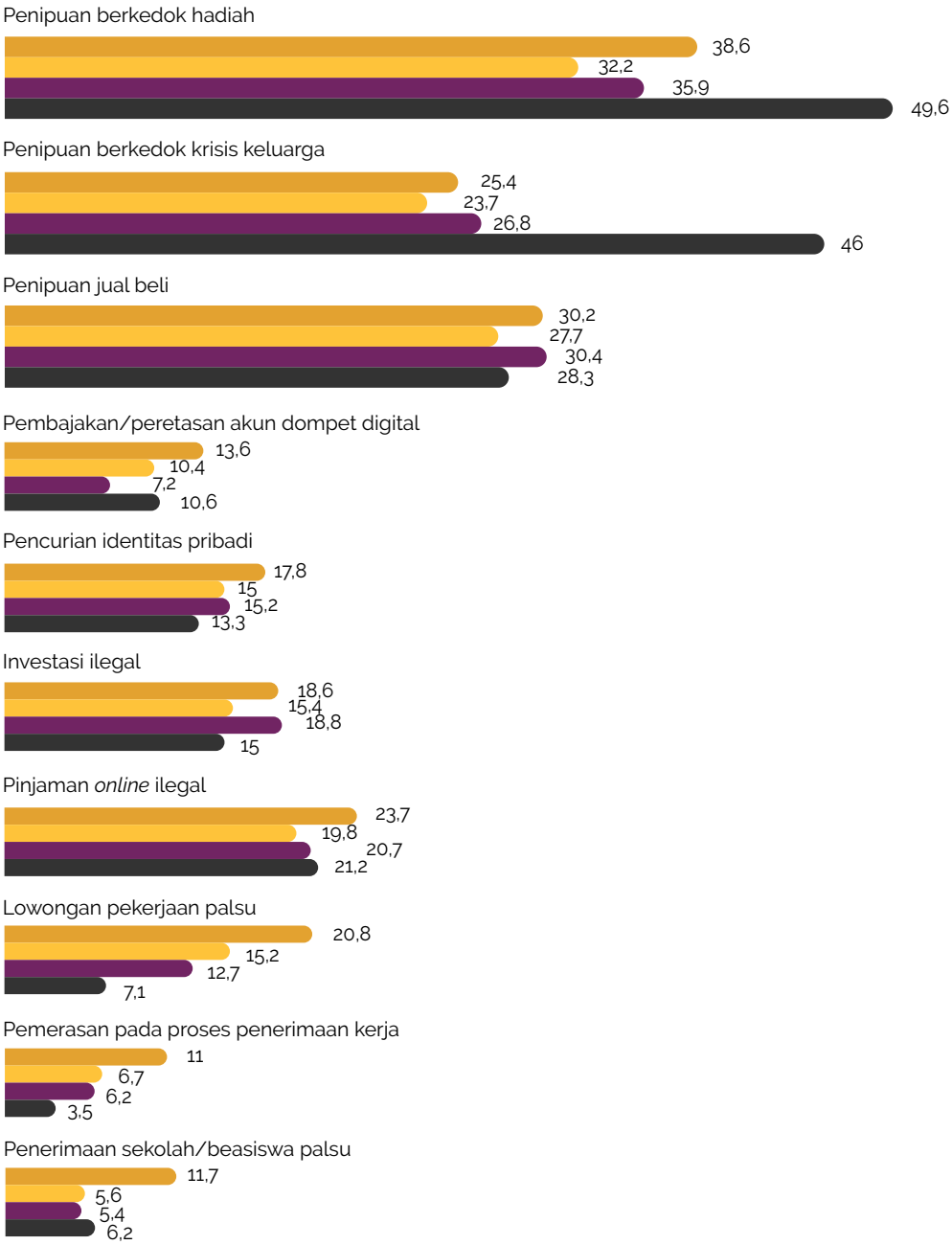
Faktanya, undian itu menjebaknya untuk mengirimkan sejumlah dana yang dimintakan dengan alasan biaya administrasi dan semacamnya.

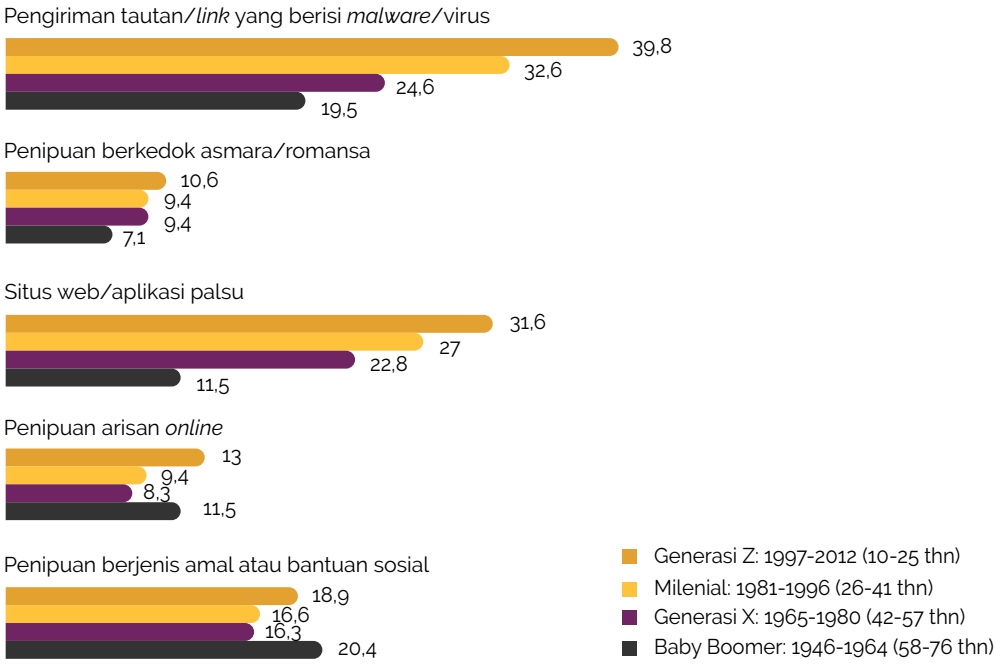
KORBAN PENIPUAN DIGITAL DAN USIA

Sangat variatifnya modus penipuan dan medium yang dipakai membuat setiap kelompok usia bisa tertipu oleh modus penipuan mana pun. Meski begitu, terdapat sebuah kecenderungan yang menunjukkan kelompok usia tertentu lebih rentan terhadap sebuah modus penipuan tertentu.

Kecenderungan ini ditampilkan dalam grafik di bawah ini, berdasarkan empat kelompok usia yang digunakan dalam riset ini, yaitu generasi Z (lahir 1997-2012), generasi Y atau Milenial (1981-1996), Gambar 4.3. Korban Penipuan Digital Berdasarkan Usia generasi X (1965-1980), dan generasi Baby Boomer (1946-1964).

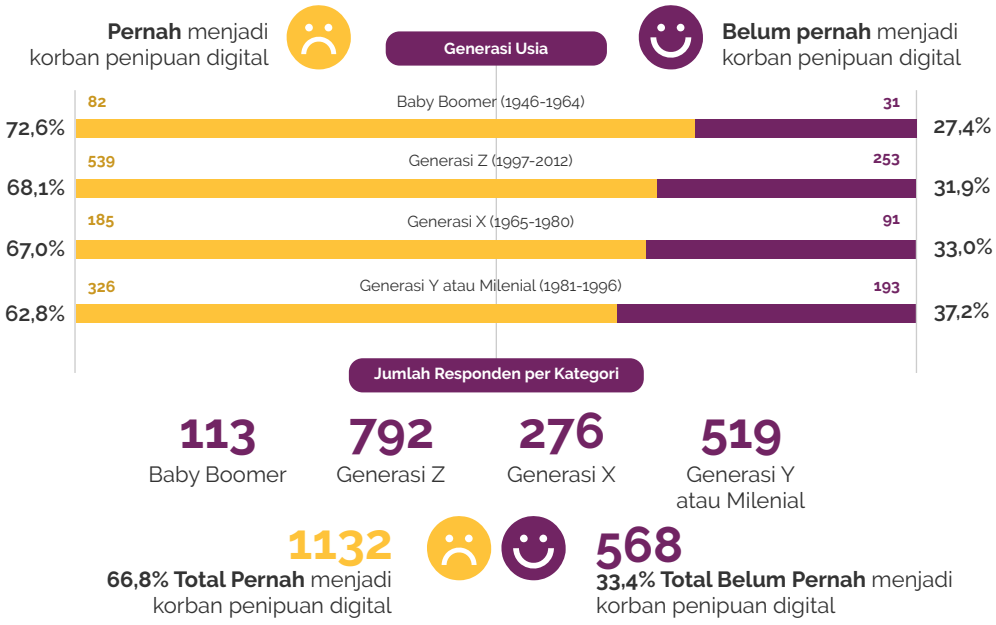
Gambar 4.3. Korban Penipuan Digital Berdasarkan Usia





Selanjutnya, riset ini juga memeringkat kelompok usia yang secara persentase paling sering menjadi korban penipuan digital, seperti tampak dalam tabel berikut.

Gambar 4.4. Korban Penipuan Digital Berdasarkan Kelompok Usia



Berdasarkan peringkat yang tampak dari tabel di atas, kategori usia yang paling banyak menjadi korban adalah Baby Boomer, yaitu sebanyak 72,6% responden dari kelompok usia tersebut, diikuti generasi Z (68,1%), generasi X (67%), dan generasi Y atau Milenial (62,8%).

Generasi Baby Boomer paling banyak tertipu oleh penipuan berkedok hadiah, yang dialami oleh hampir setengah dari mereka (49,6%), dan diikuti oleh penipuan berkedok krisis keluarga (46%). Meski demikian, mereka juga sering terjebak membuka tautan yang berisi *malware*/virus, seperti dialami oleh informan IK berikut ini.

> *"Saat itu komputer saya ngadat, lalu saya cari software yang bisa membantu untuk memperlancar. Setelah browsing, saya menemukan situs web, tapi setelah saya masuk ke dalamnya, yang terjadi malah situs itu membuat kerusakan pada dokumen-dokumen yang di komputer saya,"* **IK (58 tahun, FGD, 12 Februari 2022)**

Sementara itu, pengalaman generasi Z diwakili oleh informan AR yang terjebak penipuan berkedok hadiah seperti diuraikan di bawah ini.

AR (24 tahun, FGD, 12 Feb 2022) mengisahkan bahwa dirinya terjebak penipuan berkedok hadiah dengan menggunakan modus telepon.

> *"Dia langsung telepon, bahwa saya menang undian, banyak banget pilihannya, lalu saya pilih motor. Kalau mau ambil motor ini, saya harus transfer pulsa gitu, pulsanya nominal juga beda-beda."* **AR (24 tahun, FGD, 12 Februari 2022)**

Selanjutnya, untuk generasi X, jenis penipuan digital yang paling sering menjerat mereka adalah penipuan berkedok hadiah, yang dialami oleh 35,9% dari mereka. Contoh pengalaman ini ditunjukkan oleh dua cerita berikut.

IY (50 tahun, FGD, 9 April 2022), responden asal Bali mengisahkan bahwa dirinya terjebak penipuan jual beli karena terbuai dengan barang kebutuhan rumah tangga yang ditawarkan lebih bervariasi di toko *online* daripada berbelanja secara langsung di toko. Sayangnya, barang yang dibelinya tidak kunjung datang.

"Saya ingin rak piring, anak saya bilang bagus kalau pesan online karena banyak pilihan. Saya sudah bayar barangnya, tapi kemudian bukan barangnya yang datang, justru ojek online yang menagih katanya untuk barang itu." **(IY, 50 tahun, FGD, 9 April 2022)**

Kisah lainnya datang dari DE (44 tahun, FGD, 9 April 2022), responden survei domisili Jawa Timur mengaku ditelepon penipu berkedok krisis keluarga dengan modus yang lebih rapi dan instruktif. Ia bahkan mengaku seperti terhipnotis sehingga ia melakukan apa saja yang diinstruksikan penipu melalui telepon tersebut.

"Saya ditelepon diarahkan untuk ke ATM dan mentransfer sejumlah uang yang dia minta, instruksinya tegas banget dan saya lakukan saja mungkin karena terhipnotis." **(DE, 44 tahun, FGD, 9 April 2022)**

Yang terakhir, kelompok usia yang paling jarang menjadi korban penipuan digital adalah generasi Y atau Milenial. Meski demikian, persentase kelompok ini yang terjerat penipuan juga tinggi, salah satunya adalah penipuan jual beli, yang menjerat informan MD, seperti dalam kisah di bawah ini.

MD (27 tahun, FGD, 9 April 2022), responden domisili Papua menjadi korban penipuan jual beli di salah satu platform media sosial karena terbuai dengan promosi harga barang dan kemasan visual yang menarik.

"Saya lagi browsing baju gamis lebaran di media sosial, tergiur dengan iklan yang cantik dan harga murah, langsung check-out dan ternyata barangnya tidak dikirim sama sekali." **(MD, 27 tahun, FGD, 9 April 2022)**

Serupa dengan MD, responden inisial WA (28 tahun, 9 April 2022) asal Sulawesi Selatan juga terjerat penipuan jual beli koin untuk bermain *game* yang didapatnya dari iklan di media sosial.

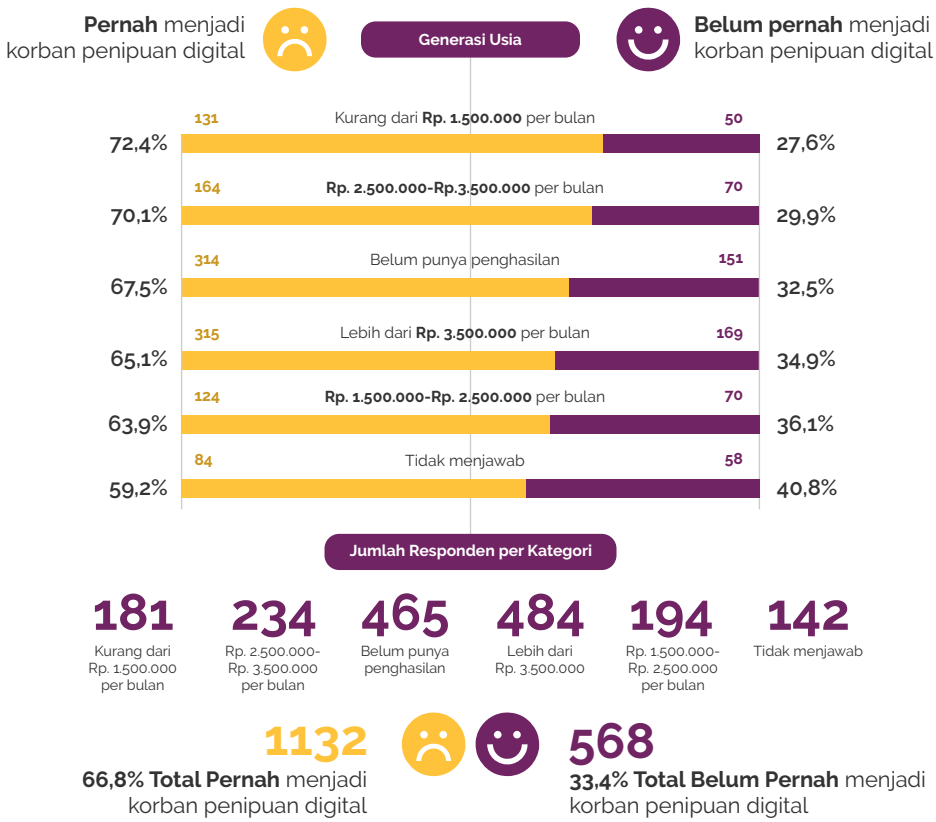
"Saya dapat iklan koin game di media sosial, saya klik dan terhubung ke aplikasi chat untuk transaksi, tetapi setelah transaksi dan nomor dihubungi kembali, tak ada balasan sama sekali." **(WA, 28 tahun, FGD, 9 April 2022)**

Dari kedua kisah responden tersebut bisa disarikan bahwa penipuan jual beli yang menargetkan kelompok generasi milenial umumnya disebabkan oleh tawaran harga barang yang lebih murah, iklan yang dirancang sedemikian rupa untuk meyakinkan, serta kadang kala muncul karena dorongan untuk memenuhi suatu kebutuhan spesifik untuk momentum tertentu.

KORBAN PENIPUAN DIGITAL DAN PENDAPATAN

Pendapatan responden dalam survei ini dibagi ke dalam enam kategori yaitu dari pendapatan yang terhitung paling tinggi (lebih dari Rp3.500.000/bulan) hingga belum punya penghasilan dan memilih untuk tidak menjawabnya. Enam kelompok ini disusun berasarkan kategori pendapatan masyarakat Indonesia yang dibuat oleh Badan Pusat Statistik. Tabel berikut menunjukkan persentase tertinggi dari penipuan digital dan pendapatan korbannya.

Gambar 4.5. Korban Penipuan Digital Berdasarkan Pendapatan

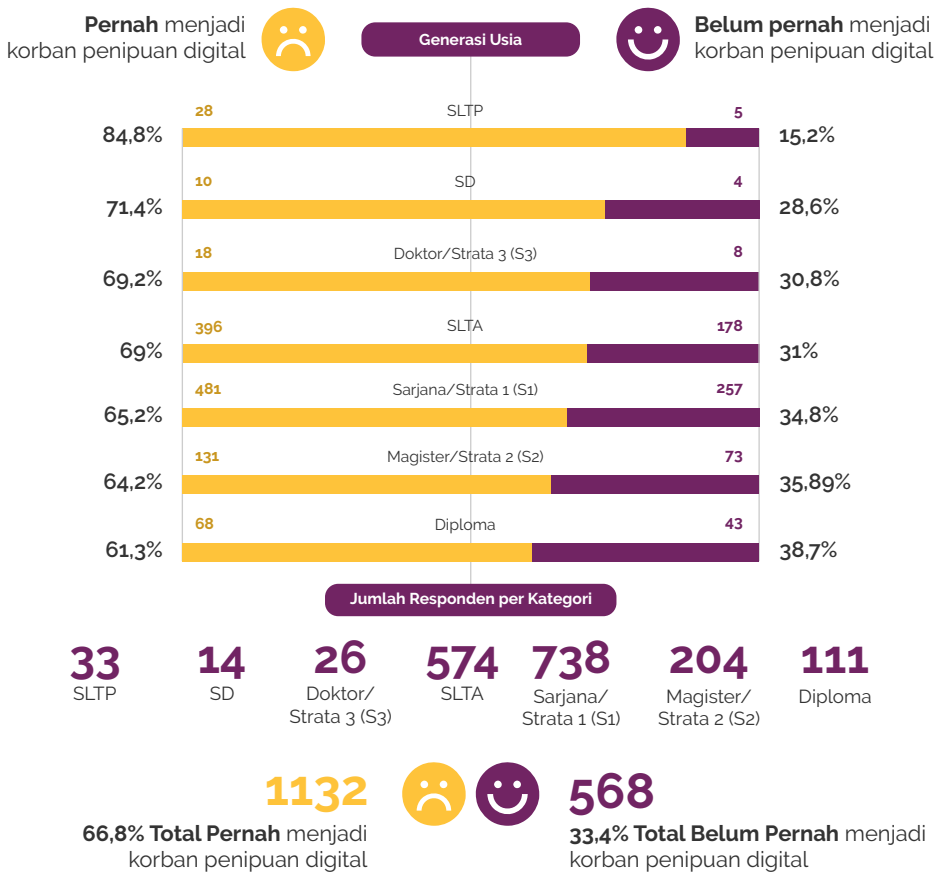


Jika dilihat dari kategori pendapatan yang pernah tertipu atau menjadi korban penipuan digital, mereka yang paling banyak menjadi korban adalah kelompok pendapatan kurang dari Rp1.500.000 per bulan, yaitu sebanyak 72,4% responden dari kelompok pendapatan tersebut. Kelompok berikutnya adalah responden dengan pendapatan antara Rp2.500.000-3.500.000 per bulan (70,1%), lalu mereka yang belum punya penghasilan (67,5%), dan kelompok responden dengan pendapatan lebih dari Rp3.500.000 per bulan.

KORBAN PENIPUAN DIGITAL DAN TINGKAT PENDIDIKAN

Riset ini mengelompokkan tingkat pendidikan responden mulai dari jenjang sekolah dasar (SD) hingga perguruan tinggi dengan gelar akademik doktoral/strata 3 (S3).

Gambar 4.6. Korban Penipuan Digital Berdasarkan Pendidikan



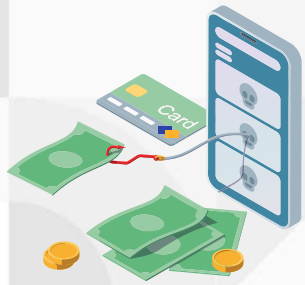
Berdasarkan tingkat pendidikan responden yang pernah menjadi korban penipuan digital, yang paling banyak menjadi korban adalah responden dengan tingkat pendidikan SLTP, yaitu sebanyak 84,8% responden dari kelompok tingkat pendidikan SLTP. Kelompok berikutnya adalah responden dengan tingkat pendidikan SD (71,4%), yang diikuti tingkat Doktoral/S3 (69,2%), SLTA (69%), Sarjana/S1 (65,2%), Magister/S2 (64,2%), dan Diploma (21.6%).

Data di atas menunjukkan bahwa latar pendidikan apa pun memiliki kerentanan yang relatif sama untuk jatuh sebagai korban. Hal ini bisa dikatakan terkait dengan kenyataan bahwa jenis penipuan digital begitu beragam dan kadang sangat canggih secara teknologi maupun modus operandi sehingga siapa pun bisa menjadi korbannya.

Dengan demikian, dari ulasan bab ini dapat disimpulkan tiga poin utama. *Pertama,* mayoritas (lebih dari setengah total responden) mengaku pernah menjadi korban penipuan digital dalam berbagai modus dan alasan terjebak sebagai korban, dengan modus paling sering adalah penipuan berkedok hadiah. *Kedua,* modus penipuan digital bisa menjerat siapa saja tanpa peduli kelompok usianya, jumlah penghasilan yang dimiliki, dan taraf pendidikan yang diraih. Olehnya itu, *ketiga,* diperlukan analisis dan pendekatan yang berbeda dan kontekstual dalam edukasi dan literasi penipuan digital sehingga masyarakat bisa terhindari dari intaian penipuan digital yang semakin lama semakin berkembang.

5

KERUGIAN PENIPUAN DIGITAL



KERUGIAN PENIPUAN DIGITAL

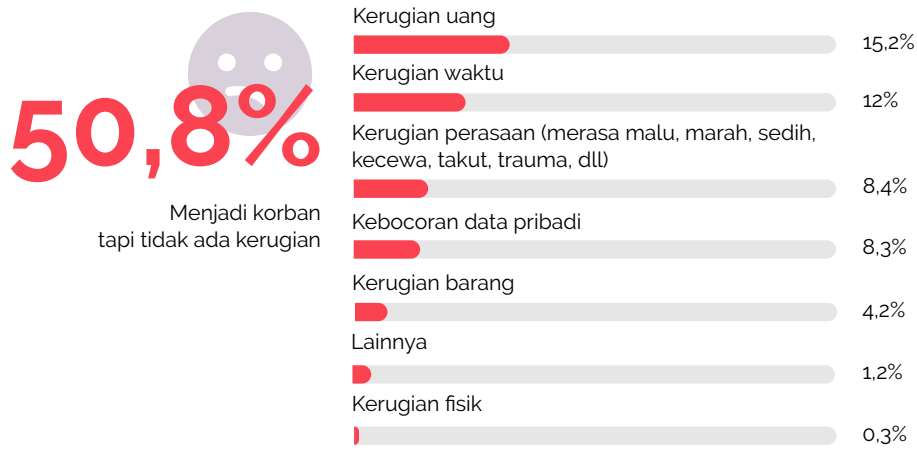
Penipuan digital bagi korbannya tentu bisa menimbulkan banyak kerugian baik yang sifatnya materil dan immateril. Kerugian materil bisa berupa uang, barang, maupun benda fisik lainnya. Sedangkan kerugian immateril bisa berupa waktu, perasaan, kebocoran data pribadi, fisik, maupun lainnya.

Komisi Eropa (2020), misalnya, membedakan dua jenis dampak utama yang dirasakan korban penipuan yakni kerugian non-finansial serta kerugian finansial. Sementara Badawi (2021) menunjukan ragam kerugian baik berupa keuangan, kebocoran data pribadi, dan informasi sensitif lainnya, serta gangguan layanan internet itu sendiri.

Dalam riset nasional ini, kerugian penipuan digital dibagi atas 8 (delapan) jenis yakni kerugian: uang, barang, kerugian fisik, kerugian waktu, kerugian perasaan, kebocoran data pribadi, tidak ada kerugian, dan kerugian lainnya.

Menariknya, riset ini menunjukkan bahwa lebih dari separuh responden (50,8%) yang menjadi korban penipuan digital menyatakan bahwa mereka "tidak mengalami kerugian".

Gambar 5.1. Jumlah Responden yang Pernah Menjadi Korban Penipuan Digital (N=1.132)

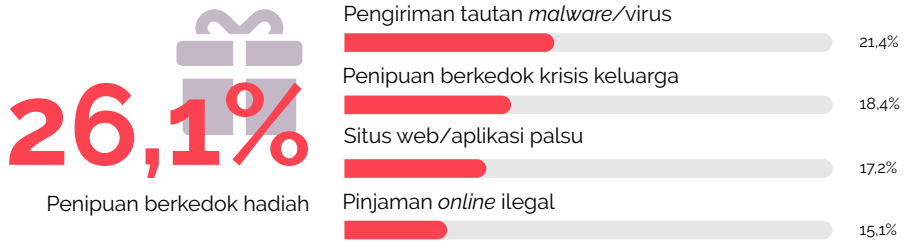


Sementara itu, di urutan kedua korban yang menyatakan mengalami kerugian uang berjumlah 15,2%. Sedangkan kerugian waktu berjumlah 12%, yang diikuti oleh kerugian perasaan (8,4%). Data selengkapnya bisa dilihat dalam Gambar 5.1.

MENJADI KORBAN TAPI TIDAK ADA KERUGIAN

Lebih separuh responden riset nasional ini menyatakan menjadi korban tapi tidak ada kerugian. Namun, jika dilihat lebih detail per jenis penipuan digital, lima urutan tertinggi jenis penipuan digital yang korbannya merasa tidak dirugikan adalah sebagai berikut.

Gambar 5.2. Jenis Penipuan Digital dan Korban yang Tidak Merasa Tidak Ada Kerugian (N=1.132)



Terlihat bahwa kerugian yang mungkin dirasakan dari lima jenis penipuan bisa kerugian finansial maupun non-finansial. Namun, temuan ini tetap menimbulkan pertanyaan: Bagaimana bisa menjadi korban penipuan digital tapi tidak merasakan kerugian sama sekali?

Untuk menjawab pertanyaan ini, serangkaian *focus group discussion* (FGD) dilakukan setelah survei dengan melibatkan 20 responden terpilih. Tujuannya adalah mengetahui lebih dalam dampak yang mereka rasakan sebagai korban penipuan. Sebagian besar mereka yang menyatakan menjadi korban tapi tidak ada kerugian beralasan telah "mengikhlaskan peristiwa itu" sebagai bagian dari "cobaan" atau "perjalanan hidup".

Berikut adalah beberapa ungkapan mereka yang menyatakan tidak mengalami kerugian meskipun menjadi korban penipuan digital.

"...mungkin memang ini bukan rezeki kita..." **(EV, 43 tahun, FGD, 19 April 2022)**

"...saya ikhlaskan saja deh..." **(BU, 60 tahun, FGD, 19 April 2022)**

Faktor keikhlasan agaknya menjadi budaya masyarakat Indonesia yang menganggap penipuan digital sebagai salah satu cobaan dalam perjalanan hidup. Tak hanya dialami oleh korban penipuan digital dalam riset ini, pengalaman korban lain yang ditulis oleh media pun juga sama. Laporan Tirto.id (Hidayat, 2021) juga menunjukkan bahwa korban penipuan digital sering kali merasa ikhlas atas kerugian penipuan digital baik kerugian finansial maupun kerugian lainnya yang ia alami bahkan terkadang lebih dari satu kali. Keikhlasan ini yang kemudian mereka anggap bahwa mereka tidak mengalami kerugian supaya tidak membebani perasaan mereka terutama karena rasa bersalah karena "terjebak" penipuan digital.

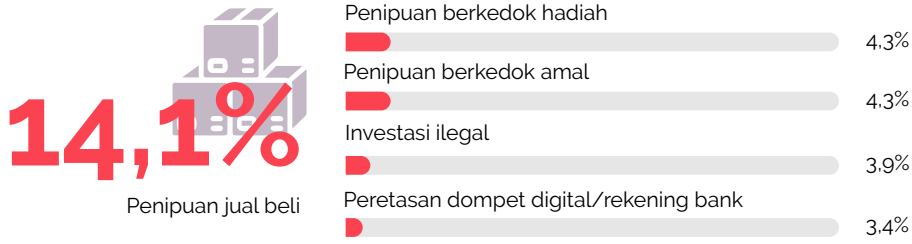
Anggapan ini kurang lebih dipengaruhi oleh prinsip agama secara umum tentang rezeki yang ada hubungannya dengan sedekah. Mereka menganggap kehilangan uang maupun barang atau benda material lainnya yang mereka alami adalah bagian dari kehilangan rezeki yang akan diganti dengan rezeki lain yang lebih besar di kemudian hari. Bahkan kadang kala korban penipuan digital merasa kurang sedekah sebelumnya sehingga menjadi korban penipuan digital adalah salah satu cara Tuhan mengingatkannya untuk lebih banyak bersedekah.

Dengan begitu, bisa dimaklumi jika sebagian responden menganggap tidak ada kerugian karena merelakan kerugian akibat penipuan digital adalah upaya untuk segera beranjak dari cobaan tersebut.

KERUGIAN UANG

Kerugian uang dari ratusan ribu rupiah hingga puluhan juta rupiah dialami oleh 14% responden survei ini. Biasanya penipuan digital yang menyebabkan kerugian adalah yang berkaitan dengan penipuan jual beli, penipuan berkedok hadiah, maupun pembajakan dompet digital termasuk rekening bank.

Gambar 5.3. Jenis Penipuan Digital dan Kerugian Uang (N=1.132)



Beberapa responden terpilih yang hadir secara luring dalam serangkaian Focus Group Discussion (FGD) menjelaskan dalam kutipan pendek kerugian uang yang mereka alami.

> *"Waktu itu lihat jualan sepatu... transfer 500... jastip nambah 50 ribu. Sudah ditransfer, chat saya di-blok, barangnya ga sampe."* **(AL, 18 tahun, FGD, 19 April 2022)**

> *"Saya sempat rugi 1 juta karena tergiur membeli hape... sudah kirimkan uang tapi barangnya tidak sampai."* **(BU, 60 tahun, FGD, 19 April 2022)**

Dari beberapa pengalaman responden sekaligus peserta FGD di atas tampak bahwa kerugian uang banyak dialami oleh korban yang usianya pun beragam dari 18 tahun hingga 60 tahun. Sebagai pembanding, kerugian uang yang dialami oleh korban penipuan digital juga banyak terjadi dalam kehidupan sehari-hari yang kemudian diberitakan oleh media. Seperti contoh kasus penipuan berkedok cinta (*romance scam*) yang dimuat di berita Kompas (Alfajri et al., 2022) yang mengalami kerugian sebanyak Rp40.000.000 dan Rp64.000.000.

Adapun contoh lain yaitu kasus aplikasi *trading* ilegal bernama Binomo (Prass, 2022), dengan korban mengalami kerugian hingga 2,5 miliar rupiah. Total uang tersebut merupakan kumpulan uang yang berasal dari keluarga, saudara, dan puluhan teman dekat korban dengan harapan dapat menghasilkan keuntungan dari *trading* di Binomo.

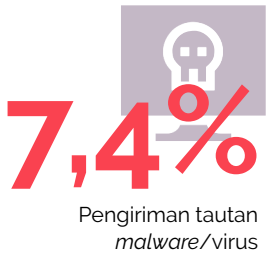
Kemudian ada pula kasus penipuan jual beli minyak goreng melalui media sosial (Linggauni, 2022), korban mengalami kerugian hingga 122 juta rupiah.

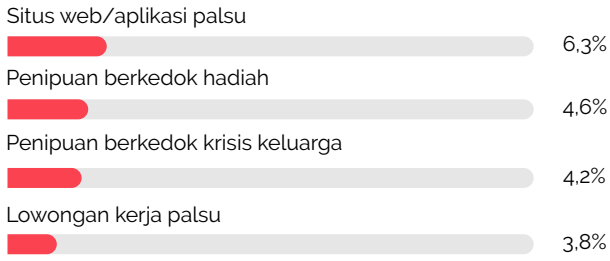
Dari apa yang dialami oleh korban penipuan digital yang menjadi responden riset nasional ini maupun korban lain yang diberitakan media, tampak bahwa kerugian uang terjadi dalam berbagai modus penipuan digital dengan beragam medium serta menimpa korban dengan bervariasi usia.

KERUGIAN WAKTU

Sedangkan kerugian waktu dirasakan oleh korban penipuan karena waktu mereka menjadi berkurang akibat harus melakukan banyak hal setelah menjadi korban penipuan digital.

Gambar 5.4. Jenis Penipuan Digital dan Kerugian Waktu (N=1.132)





Waktu yang berkurang itu digunakan untuk meminta bantuan dari teman atau keluarga atau pemangku kepentingan yang lain terutama mengupayakan kembalinya uang, barang atau benda lain yang hilang. Selain itu waktu juga berkurang karena korban penipuan digital sering kali terganggu perasaannya, sebagaimana pernyataan beberapa responden sekaligus peserta FGD riset ini.

> *"Itu kan menghabiskan waktu kita untuk melaksanakan pelaporan. Tapi tidak ada follow up-nya"* **(KT, 58 tahun, FGD, 19 April 2022)**

> *"bingung kita mau ngapain, setelah kita ketipu tuh bingung mau ngapain."* **(YG, 23 tahun, FGD, 19 April 2022)**

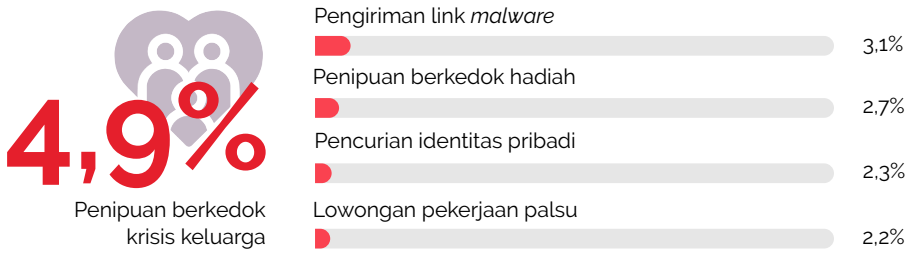
Kerugian waktu seperti diceritakan dua informan di atas terkadang tidak dirasakan karena tidak langsung tampak seperti halnya kerugian uang maupun kerugian benda lain yang terlihat secara fisik.

Namun, korban dirugikan waktunya untuk merespons penipuan digital yang menimpanya. Pilihan untuk melaporkan maupun tidak ke pihak yang berwajib membuat kehilangan waktu dalam proses tersebut. Bahkan, dari laporan dari Media Konsumen (Sulaeman, 2022), calon korban penipuan digital pun mengalami kerugian waktu ketika melaporkan persoalan yang dihadapinya. Acapkali laporan calon korban ini tidak ditangani dengan cepat padahal risikonya tinggi.

KERUGIAN PERASAAN

Merasa malu, marah, sedih, kecewa, takut, trauma, adalah beragam perasaan yang dialami oleh korban karena tidak ada seorang pun ingin menjadi korban penipuan digital.

Gambar 5.5. Jenis Penipuan Digital dan Kerugian Perasaan (N=1.132)



Bahkan sebagian responden yang menjadi peserta FGD yang dilakukan dengan tim peneliti, bahwa sebagai korban penipuan digital mereka merasa menyesal karena termakan bujuk rayu pelaku penipuan digital. Mereka juga merasa gagal mengkritisi pesan penipuan digital sekaligus merasa gagap mempraktikkan aman bermedia digital.

Perasaan yang beragam ini timbul karena korban merasa lengah sehingga celah kejahatan penipuan digital bisa menimpanya.

"...pengenlah untuk melaporkan, tapi sudah kadung malu..."
(RN, 27 tahun, FGD, 19 April 2022)

"Waktu tau oh ternyata ini penipuan, saya jengkel sebenarnya."
(YD, 28 tahun, FGD, 19 April 2022)

"Marah, kecewa hahaha saya ditipu. Saya juga menyalahi diri sendiri, 'Bodoh sih saya ini kenapa kok ketipu.'"
(BU, 60 tahun, FGD, 19 April 2022)

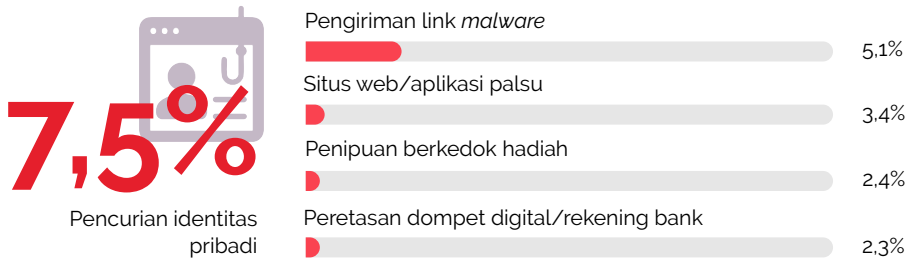
Dari beberapa pernyataan responden yang menjadi peserta FGD dalam riset ini, terlihat bahwa kerugian perasaan membuat korban menyesali dirinya terperangkap dalam penipuan digital dan menyalahkan dirinya sendiri. Perasaan lain yang muncul antara lain malu, jengkel, kecewa, hingga marah.

Kasus yang diterbitkan Detik.com (Pinandhita, 2022) juga menunjukkan kerugian perasaan korban penipuan digital berkedok asmara. Korban yang ditipu oleh teman kencannya di suatu aplikasi kencan merasa trauma untuk memulai hubungan baru akibat ditinggalkan *(ghosting)* oleh teman kencan virtualnya.

KEBOCORAN DATA PRIBADI

Terkadang korban melihat kebocoran data pribadi bukan sebagai kerugian karena ini bukan kerugian yang langsung dirasakan atau nyata. Namun, ketika diminta mengisi kuesioner, mereka paham bahwa kebocoran data pribadi adalah salah satu kerugian dalam penipuan digital, yang akibatnya bisa sangat nyata.

Gambar 5.6. Jenis Penipuan dan Kebocoran Data Pribadi (N=1.132)



Dalam riset ini, korban pencurian identitas adalah kelompok korban yang paling merasakan kerugian berupa kebocoran data pribadi

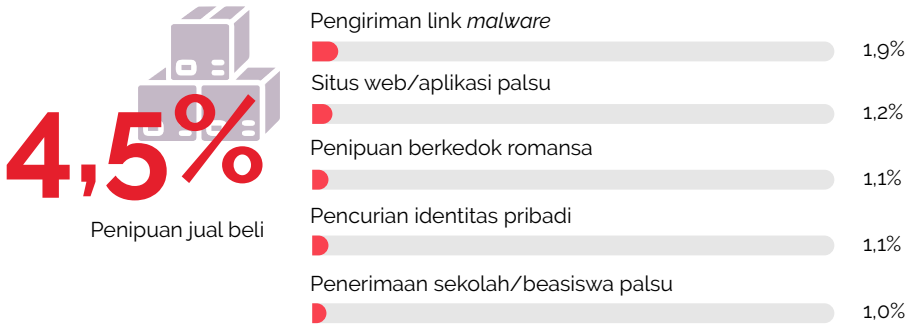
> *"Ada yang menggunakan nama saya dan menggunakan foto profil saya, dan dia nge-chat....banyak orang untuk meminjam uang."*
> **(YG, 23 tahun, FGD, 19 April 2022)**

Terkait dengan kebocoran data pribadi, laporan Kompas (Gatra, 2021) pernah merilis berita kasus pinjaman *online* di mana korban mengalami tindakan penyebarluasan informasi pribadi ke publik atau disebut dengan istilah *doxing*. Data yang disebarluaskan pelaku adalah foto korban yang sedang memegang Kartu Tanda Penduduk (KTP) miliknya ketika mendaftar ke aplikasi pinjol. Foto tersebut lalu disandingkan dengan foto perempuan tanpa busana yang seolah-olah merupakan foto korban. Foto ini disebarluaskan di media sosial dengan narasi menerima pesanan untuk melayani transaksi seksual atau dengan istilah *open booking order* (open BO). Kasus lain adalah pesan spam melalui aplikasi *chat* yang mencantumkan alamat lengkap korban, dengan pelaku meng-atasnamakan dirinya sebagai pihak lokapasar ternama (Nadiroh, 2021)

KERUGIAN BARANG

Kerugian barang dialami paling banyak oleh korban penipuan jual beli (4,5%) dibandingkan dengan jenis penipuan lainnya sebagaimana terlihat dalam Gambar 5.7.

Gambar 5.7. Jenis Penipuan Digital dan Kerugian Barang (N=1.132)



Dalam FGD yang dilakukan sebelum survei, salah seorang peserta yang merupakan penjual kue kering mengalami kerugian barang karena ditipu pembelinya.

> *"Kue kering sebanyak itu total hampir 3 juta... Karena ini ada pengiriman jauh, saya minta DP-nya terlebih dahulu. Ee lalu, ee pas saya minta DP, 'Nggak usah, Mbak. Nggak usah pakai DP DP, langsung saya bayar semua aja', katanya gitu.... saya tahunya dia pakai m-banking pengiriman palsu. .... Uang tidak masuk. Padahal kue-kuenya sudah saya pack, sudah siap kirim."* **(ND, 28 tahun, FGD, 12 Februari 2022)**

Sementara itu, korban lain yang mengalami kerugian barang adalah dari sisi pembeli yang ditipu penjualannya.

> *"Kemarin waktu bulan puasa itu ngambil mukenah sekitar 17 pcs, yang dia kirim itu cuma 5 pcs, yang lainnya itu dia nggak kirim, lalu nomor saya dia blokir"* **(HD, 52 tahun, FGD, 12 Februari 2022)**

Dari dua pengalaman di atas, tampak bahwa kerugian barang dalam penipuan jual beli tak hanya bisa menimpa pembeli namun juga penjual.

Meskipun begitu, penipuan jual beli lebih banyak memakan korban yang berposisi pembeli sebagaimana ditulis Media Konsumen (Barasa, 2022). Korban melakukan pembelian tas bermerek seharga Rp2.300.000 melalui fitur *live streaming* di salah satu aplikasi lokapasar terkenal.

Setelah paket tas diterima, ternyata tas yang dikirim merupakan produk palsu dan tidak sesuai dengan klaim pelaku pada saat *live streaming*.

KERUGIAN FISIK

Meskipun hanya 15 responden (0.4%) yang mengisi pengalaman kerugian fisik termasuk melukai diri sendiri, hal ini menunjukkan bahwa penipuan digital bisa mengakibatkan korbannya melakukan *self-harm*.

Gambar 5.8. Jenis Penipuan dan Kerugian Fisik (N=1.132)

2
orang
1,>%

- Pencurian identitas pribadi
- Penerimaan sekolah/beasiswa palsu
- Pengiriman berisi *malware*/virus
- Situs web/aplikasi palsu

1
orang
1,>%

- Penipuan berkedok krisis keluarga
- Penipuan jual beli
- Peretasan dompet digital/rekening bank
- Investasi ilegal
- Lowongan kerja palsu
- Pemerasan/penerimaan lowongan kerja
- Penipuan berjenis amal

0
orang

- Penipuan berkedok hadiah
- Pinjaman *online* ilegal
- Penipuan berkedok asmara
- Penipuan arisan *online*

Meskipun dalam FGD yang dilakukan tim penelitian tidak ditemukan pernyataan langsung tentang kerugian fisik, kasus kerugian fisik bisa dialami oleh korban penipuan digital. Salah satunya adalah pemberitaan Tribun (Juliati, 2022) yang melaporan seorang korban pinjaman *online* ilegal yang tak hanya mengalami kerugian uang ratusan juta rupiah namun juga kerugian fisik dengan menyusutnya berat badannya hingga 12 kg

6

RESPONS KORBAN PENIPUAN DIGITAL

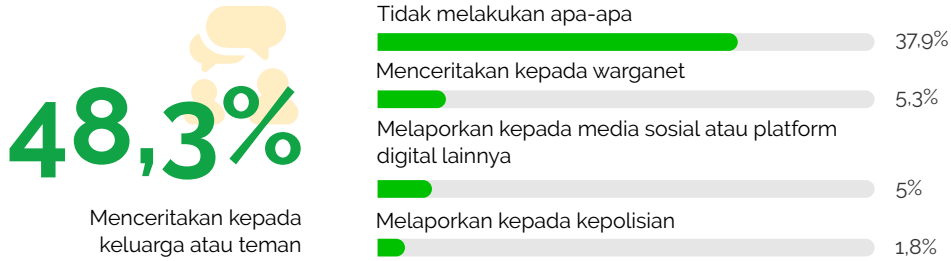
RESPONS KORBAN PENIPUAN DIGITAL

Tidak seorang pun ingin menjadi korban penipuan digital, tak peduli latar belakang usia, pendapatannya maupun pendidikannya. Meskipun begitu, karena beragam faktor, baik yang berasal dari kelalaian diri sendiri maupun kelengahan orang lain, korban penipuan digital sering kali tak bisa menghindari beragam modus kejahatan siber yang paling populer ini.

Riset nasional ini juga menanyakan pada seluruh responden melalui survei maupun FGD mengenai respons mereka setelah menyadari bahwa mereka menjadi korban penipuan digital.

Dari seluruh korban penipuan digital yang berjumlah 1.132 responden, respons atau tindakan terbanyak yang mereka lakukan adalah menceritakan kepada keluarga atau teman (48,3%), tidak melakukan apa-apa (37,9%), menceritakan kepada warganet (5,3%), melaporkan kepada media sosial atau platform digital lainnya (5%), dan melaporkan kepada kepolisian (1,8%).

Gambar 6.1. Respons Korban Penipuan Digital (N=1.132)

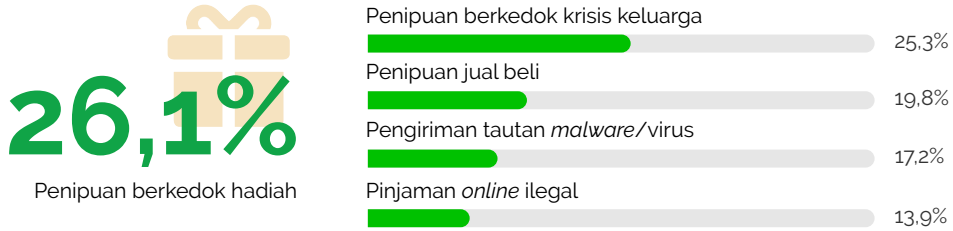


Meski lapor ke kepolisian hanya menjadi pilihan 1,8% responden, sebanyak 97,3% responden menganggap kepolisian dan aparat penegak hukum lainnya sebagai pihak yang paling bertanggung jawab untuk mencegah dan menangani penipuan digital, yang diikuti oleh pemerintah (96,2%), perusahaan terkait (93,3%), organisasi masyarakat sipil atau komunitas-komunitas di masyarakat (85,5%), dan perguruan tinggi (81,9%).

MENCERITAKAN KEPADA KELUARGA ATAU TEMAN

Menceritakan kepada keluarga atau teman merupakan respons terbanyak yang dipilih oleh lebih dari separuh responden. Pilihan ini masuk akal karena korban butuh segera mendapatkan bantuan atau dukungan dari orang-orang terdekatnya baik itu keluarga maupun teman. Bagi korban, hanya keluarga dan teman yang bisa mereka percaya bisa membantu dan menjaga rahasia mereka. Kepercayaan ini penting karena korban mengalami berbagai perasaan seperti kecewa, jengkel, marah, hingga malu sehingga tak ingin kejadian yang tak mengenakkan ini diketahui oleh orang banyak.

Gambar 6.2. Menceritakan Kepada Keluarga atau Teman dan 5 Modus Penipuan Digital Terbanyak (N=1.132)



Gambar 6.2 menunjukkan korban penipuan berkedok hadiah paling banyak (26,1%) menceritakan kasus penipuan berkedok hadiah yang menimpanya. Sementara empat modus lainnya yang paling banyak ditemukan secara berurutan adalah: penipuan berkedok krisis keluarga, penipuan jual beli, pengiriman tautan *malware*/virus, dan pinjaman *online* ilegal.

Beberapa informan FGD menyampaikan pengalaman mereka dibantu teman ketika mengalami penipuan digital.

> *"...cerita ke teman. Saya kena penipuan kayak gini gini gini, akhirnya teman saya bantu."* **(EV, 43 tahun, FGD, 19 April 2022)**

> *"...saya cerita ke teman saya... di-blokirkan, lalu bikin akun baru"* **(BU, 60 tahun, FGD, 19 April 2022)**

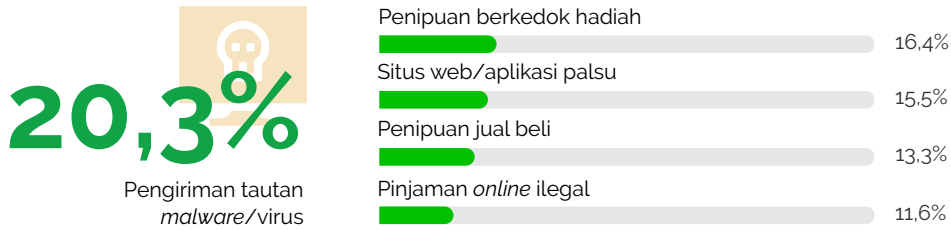
Kutipan di atas menunjukkan bahwa tidak semua korban mampu secara teknis dan psikologis berhadapan dengan berbagai langkah ikutan mengatasi berbagai dampak dari penipuan digital.

Bisa jadi, pengetahuan praktis mengenai apa yang harus dilakukan setelah menjadi korban penipuan digital tidak cukup memadai untuk setidaknya melakukan berbagai langkah mencegah penipuan digital terulang kembali.

TIDAK MELAKUKAN APA-APA

Tidak melakukan apa-apa merupakan respons terbanyak kedua yang dipilih responden saat menyadari dirinya menjadi korban penipuan digital. Modus penipuan digital terbanyak yang mengakibatkan korban penipuan digital tidak melakukan apa-apa adalah pengiriman tautan *malware*/virus (20,3%), yang diikuti penipuan berkedok hadiah, situs web/aplikasi palsu, penipuan jual beli, dan pinjaman lainnya.

Gambar 6.3. Tidak Melakukan Apa-apa dan 5 Modus Penipuan Digital Terbanyak (N=1.132)



Beberapa pernyataan responden terpilih yang menjadi FGD menunjukkan berbagai alasan mereka tidak melakukan apa-apa meskipun menjadi korban penipuan digital

"Malu sama keluarga, malu sama temen-temen, jadi saya diem-diem aja." **(RN, 27 tahun, FGD, 19 April 2022)**

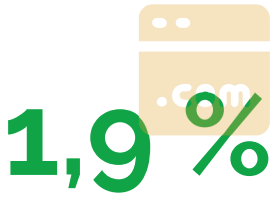
"...saya belum melapor ke polisi juga, terus saya belum minta tolong ke teman. Yaudahlah, biar aja. Mudah-mudahan nanti diganti...)" **(EV, 43 tahun, FGD, 19 April 2022)**

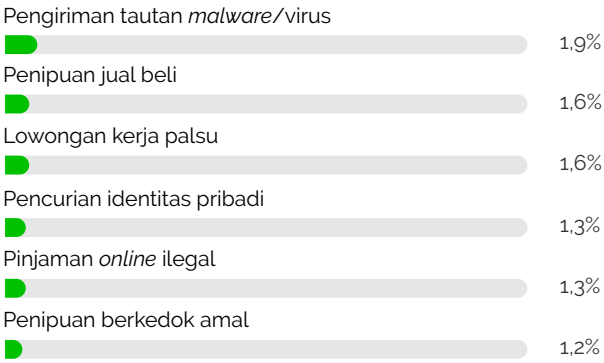
Dari beberapa pernyataan di atas, tampak bahwa malu dan ikhlas menjadi alasan responden terpilih untuk tidak melakukan apa-apa.

MENCERITAKAN KEPADA WARGANET

Pilihan respons terbanyak ketiga korban penipuan digital dalam riset ini adalah menceritakan pada warganet.

Gambar 6.4. Menceritakan Kepada Warganet dan 5 Modus Penipuan Digital Terbanyak (N=1.132)





Penipuan situs web/aplikasi palsu merupakan modus terbanyak yang membuat responden memilih menceritakan kepada warganet diikuti oleh empat modus terbanyak lainnya seperti terlihat dalam Gambar 6.4.

Biasanya alasan untuk menceritakan pada warganet adalah untuk berbagi pengalaman sehingga warganet bisa belajar dari pengalaman tersebut dan menghindarinya.

"Kita share.....tentang ciri-ciri dari penipuan tersebut....biar teman-teman yang lain kalau sekiranya dapat eee dapat email tentang pekerjaan tersebut, ya nggak usah ditanggapi aja" **(SY, 31 tahun, FGD, 19 April 2022)**

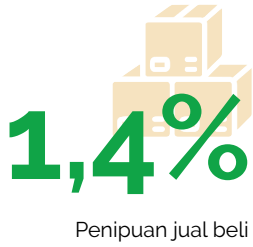
"Tapi ketika...akun saya dikloning, gitu, saya langsung sharing ke media sosial agar tidak ada yang tertipu." **(YG, 23 tahun, FGD, 19 April 2022)**

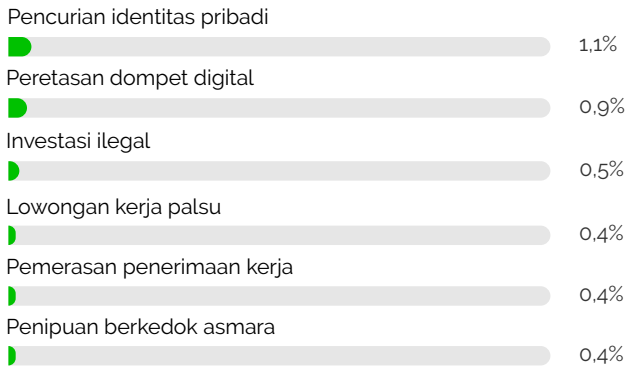
Pilihan ini tentu saja bisa dimaklumi karena korban ingin berpartisipasi untuk mencegah penipuan digital. Hal sama juga dilakukan oleh figur publik Luna Maya yang menceritakan kronologi penipuan digital yang menimpa dirinya oleh oknum yang tidak bertanggung jawab melalui media sosialnya (Arifin, 2022).

MELAPORKAN KEPADA KEPOLISIAN

Melaporkan kepada Kepolisian tak banyak dilakukan oleh responden riset nasional ini. Terlihat dalam Gambar 6.5 modus terbanyak yang dilaporkan korban adalah penipuan jual beli (1,4%).

Gambar 6.5. Melaporkan Kepada Polisi dan 5 Modus Penipuan Digital Terbanyak (N=1132)





Salah satu responden terpilih menyatakan bahwa ia sempat memilih untuk melaporkan ke polisi tapi tidak merasa terbantu.

> *"...udah saya langsung jalan ke kepolisian, Tapi ya udah gak ada apa-apa."* **(NU, 53 tahun, FGD, 19 April 2022)**

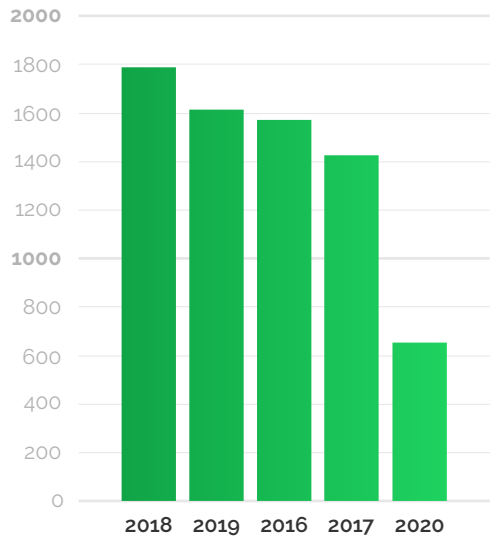
Sementara itu, menurut laporan Barometerrakyat.com (Sahrul, 2022), seorang korban telah mengalami penipuan sebesar Rp18.000.000 sebagai setoran arisan *online,* tetapi uang yang telah disetorkan tidak kembali dan korban langsung melaporkan pemilik arisan *online* tersebut ke Satuan Reserse Kriminal (Satreskrim) Polresta Tanjung Pinang. Atau di lain kasus, seperti dikutip dari Tribunjabar.id, korban dugaan penipuan investasi dengan total kerugian sebesar 565 miliar rupiah melaporkan kasusnya ke Polda Metro Jaya (Ravianto, 2022).

Namun begitu, sama halnya dengan temuan riset ini, Laporan Tirto.id (Hidayat, 2021) juga menunjukkan bahwa lapor ke polisi jarang dilakukan oleh korban penipuan digital. Dari sedikit korban penipuan digital yang melaporkan ke polisi, tindak lanjut dari polisi bisa dikatakan tidak ada, sehingga mereka merasa tidak mendapatkan keuntungan apa-apa dengan melapor ke polisi.

Pengalaman sekelompok kecil korban yang merasa tidak puas terhadap pelayanan polisi dalam menindaklanjuti laporan penipuan digital ini kemudian dibagikan ke teman maupun saudara atau bahkan ke media sosial. Dengan begitu, ada semacam "pengetahuan umum" bahwa tidak ada gunanya lapor ke polisi jika menjadi korban penipuan digital.

Maraknya pengalaman korban yang kurang mendapatkan tindak lanjut dari polisi ini menjadi contoh korban-korban selanjutnya untuk tidak melapor atau mengikhlaskan kasusnya. Tren melapor kepada Polri terkait penipuan digital setidaknya mengalami penurunan dalam lima tahun terakhir (2016-2020). Berikut data dari Polri yang dilaporkan oleh Databoks (Pusparisa, 2020):

Gambar 6.6. Jumlah Laporan Penipuan Digital Per Tahun dari Kepolisian Republik Indonesia



Sumber: Kepolisian Republik Indonesia (Polri) (2020)

Bahkan, dalam FGD riset ini, ada keengganan lapor ke polisi di antara informan karena ada anggapan bahwa laporan yang diproses hanyalah korban penipuan digital yang kerugian ratusan juta rupiah ke atas dan atau dilaporkan oleh orang terkenal atau figur publik.

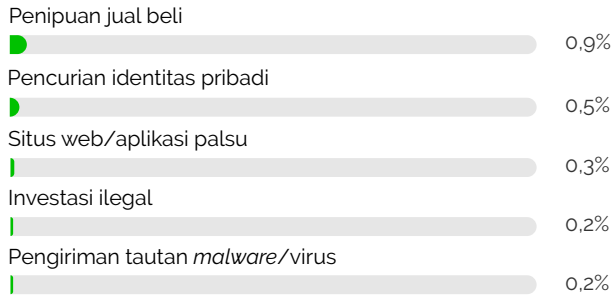
MELAPORKAN KEPADA LEMBAGA OTORITAS TERKAIT

Korban peretasan dompet digital/rekening bank terbukti yang paling banyak (1,1%) melaporkan lembaga terkait dibandingkan dengan korban penipuan jual beli maupun pencurian identitas pribadi.

Gambar 6.7. Melaporkan Kepada Lembaga/Otoritas Terkait dan 5 Modus Penipuan Digital Terbanyak (N=1.132)

1,1%

Peretasan dompet digital/ rekening bank



Di semua jenis penipuan digital, meskipun sedikit, ada upaya melaporkan ke lembaga/otoritas terkait seperti OJK, Bappebti, dan lembaga perbankan. Seperti kasus penipuan berkedok investasi yang dilaporkan oleh Detik.com (Fadhillah, 2022), kuasa hukum korban yaitu Ibrahim Sumantri mengatakan pihaknya telah melaporkan kasusnya ke Badan Pengawas Berjangka Komoditi (Bappebti) Kementerian Perdagangan.

MELAPORKAN KEPADA LEMBAGA PEMERINTAH ATAU KEMENTERIAN

Melaporkan pada lembaga pemerintah atau kementerian adalah pilihan respons yang tak banyak dilakukan responden riset ini.

Gambar 6.8. Melaporkan Kepada Lembaga Pemerintah atau Kementerian dan Modus Penipuan Digital (N=1.132)

0,4%
4 responden

- Penipuan jual beli
- Pencurian identitas pribadi

0,3%
3 responden

- Penerimaan sekolah/beasiswa palsu
- Pengiriman tautan *malware*/virus

0,2%
2 responden

- Penipuan berkedok hadiah
- Investasi ilegal
- Lowongan kerja palsu
- Penipuan berkedok amal

0,1%
1 responden

- Peretasan dompet digital/rekening bank
- Pinjaman *online* ilegal
- Situs web/aplikasi palsu

0%

0 responden

- Penipuan berkedok krisis keluarga
- Pemerasan penerimaan kerja
- Penipuan berkedok asmara
- Penipuan arisan *online*

MELAPORKAN KEPADA LEMBAGA BANTUAN HUKUM

Melaporkan pada lembaga bantuan hukum tak banyak dilakukan oleh responden riset nasional ini. Korban penipuan berkedok hadiah dan pinjaman *online* ilegal yang paling banyak melaporkan pada lembaga bantuan hukum.

Gambar 6.9. Melaporkan Kepada Lembaga Bantuan Hukum dan Modus Penipuan Digital (N=1.132)

0,2%

2 responden

- Penipuan berkedok hadiah
- Pinjaman *online* ilegal

0,1%

1 responden

- Penipuan berkedok krisis keluarga
- Penipuan jual beli
- Peretasan dompet digital
- Pencurian identitas pribadi
- Investasi ilegal
- Pengiriman *link malware*
- Penipuan berjenis amal atau bantuan sosial

0%

0 responden

- Lowongan kerja palsu
- Pemerasan penerimaan kerja
- Penerimaan sekolah atau beasiswa palsu
- Penipuan berkedok romansa atau asmara
- Situs web/aplikasi palsu
- Penipuan arisan *online*

Terangkum dalam redaksi Okenews.com, pada Senin, 18 Oktober 2021, Lembaga Bantuan Hukum Dewan Pengacara Nasional (LBH DPN) Indonesia secara resmi membuka Pusat Pengaduan Nasional Korban Pinjol Ilegal (Okezone, 2021). Adapun korban pinjol pertama yang melaporkan kasusnya kepada LBH terjadi pada tahun 2018 (Arbi, 2021).

MELAPORKAN KEPADA LEMBAGA PERLINDUNGAN WARGA ATAU KONSUMEN

Respons korban paling sedikit dalam studi ini adalah melaporkan pada lembaga perlindungan warga atau konsumen. Hanya dua responden yang melaporkan ke lembaga perlindungan warga atau konsumen terkait penipuan jual beli yang menimpanya.

Gambar 6.10. Melaporkan Kepada Lembaga Perlindungan Warga atau Konsumen (N=1.132)

0,1%

1 responden

- Penipuan jual beli
- Situs web/aplikasi palsu

0%

0 responden

- Penipuan berkedok hadiah
- Penipuan berkedok krisis keluarga
- Peretasan dompet digital
- Pencurian identitas pribadi
- Investasi ilegal
- Pinjaman *online* ilegal
- Lowongan kerja palsu
- Pemerasan penerimaan kerja
- Penerimaan sekolah/beasiswa palsu
- Pengiriman *link malware*
- Penipuan berkedok asmara atau romansa
- Penipuan arisan *online*
- Penipuan berjenis amal atau bantuan sosial

7

REKOMENDASI PENCEGAHAN DAN PENANGANAN PENIPUAN DIGITAL

REKOMENDASI PENCEGAHAN DAN PENANGANAN PENIPUAN DIGITAL

Bab ini membahas rekomendasi yang meliputi enam bahasan, yaitu (1) pencegahan penipuan digital, (2) penanganan penipuan digital, (3) pihak yang dinilai responden terpercaya dalam memberikan informasi pencegahan, (4) pihak yang dianggap responden bertanggung jawab dalam mencegah dan menangani penipuan digital, (5) rekomendasi pencegahan menurut korban penipuan digital, dan (6) rekomendasi penanganan menurut korban penipuan digital.

Dua bahasan pertama merujuk pada hasil olah data keseluruhan responden (N=1.700 responden), sementara dua pokok bahasan terakhir berdasarkan pada hasil olah data responden yang pernah menjadi korban (N=1.132). Pembedaan ini perlu dilakukan untuk memperlihatkan perbandingan persebaran data antara yang umum dan yang khusus (korban), yang akan berguna dalam merencanakan kebijakan atau program dan menentukan target sasaran nantinya. Pembahasan rekomendasi ini melibatkan banyak entitas, yaitu pemerintah, kepolisian, sektor swasta, institusi pendidikan dan warga masyarakat.

PENCEGAHAN PENIPUAN DIGITAL

Berbagai usulan disampaikan responden untuk dapat menanggulangi kasus penipuan digital. Temuan survei menunjukkan bahwa upaya pencegahan penipuan digital yang dianggap penting oleh responden, secara berurutan, sebagai berikut:

1. Peningkatan sistem keamanan dan perlindungan data pribadi (98,1%)
2. Kepastian hukum bagi penanganan penipuan digital (98,1%)
3. Publikasi kasus terkini dan modus operandi penipuan digital (97,2%)
4. Edukasi atau pelatihan tentang keamanan digital (97%)
5. Ketersediaan situs web dan aplikasi dari pihak berwenang untuk bisa mengecek validitas penjual (96,7%)
6. Kampanye publik agar warga berhati-hati dan tips cara menghindari penipuan (95,9%)

Ada dua upaya pencegahan yang tampaknya sama penting bagi responden, yaitu peningkatan sistem keamanan dan perlindungan data pribadi dan kepastian hukum bagi penanganan *online*.

Meski demikian, jika ditelusuri lebih mendalam dengan melihat bobot jawaban responden (dari banyaknya yang memberikan jawaban "sangat penting") maka peningkatan sistem keamanan dan perlindungan data pribadi dapat menjadi prioritas utama. Secara lengkap, berikut grafik yang menunjukkan distribusi data tersebut.

Gambar 7.1. Program Pencegahan Penipuan Digital (N=1.700)

- **98,1%** Peningkatan sistem keamanan dan perlindungan data pribadi
- **98,1%** Kepastian hukum bagi penanganan penipuan digital
- **97,2%** Publikasi kasus terkini dan modus operandi penipuan digital
- **97%** Edukasi atau pelatihan tentang keamanan digital
- **96,7%** Ketersediaan situs web dan aplikasi dari pihak berwenang untuk bisa mengecek validitas penjual
- **95,9%** Kampanye publik agar warga berhati-hati dan tip cara menghindari penipuan

Penipuan digital merupakan tindakan penipuan yang dimediasi (diantarai) oleh perangkat dan jaringan komunikasi digital, seperti media sosial dan berbagai aplikasi termasuk aplikasi belanja daring. Oleh karena itu, sistem keamanan perangkat komunikasi menjadi perhatian utama responden untuk mencegah terjadinya penipuan.

Meskipun keamanan perangkat ini dapat diatasi dengan meningkatkan kecakapan digital dan kesadaran individu untuk lebih berhati-hati dalam bermedia, tuntutan terhadap keamanan perangkat di sini lebih mengarah pada para pemilik dan penyedia platform digital. Temuan survei menunjukkan, responden yang berpendidikan S3 yang diasumsikan memiliki pemahaman yang lebih baik terhadap perangkat/media digital masih juga menjadi korban penipuan daring. Kasus yang paling banyak adalah mereka menjadi korban penipuan berhadiah (38,5% atau berjumlah 5 dari 26 orang).

Para pemilik platform memiliki peran penting dalam mencegah penipuan digital. Aspek keamanan dan privasi data seharusnya menjadi komponen utama yang menjadi perhatian dalam proses pengembangan dan pemberian layanan digital. Ada sejumlah kelalaian yang dilakukan pemilik dan berakibat pada ancaman keamanan pengguna, termasuk kebocoran data pribadi.

Mengutip pernyataan Ricky Setiadi, seorang AVP Information Security sebuah lokapasar, ada banyak kasus pemilik atau pengembang platform melakukan kesalahan dalam proses pengembangan atau pemeliharaan layanan digital (Eka, 2020). Sebagai contoh, pengembang lalai dalam menerapkan enkripsi untuk penggunaan *username* dan *password.* Termasuk juga, pengembang tidak menerapkan penyimpanan *private key* sehingga tidak aman serta penggunaan *account default* untuk sistem yang digunakan. Kelalaian terkait pemeliharaan misalnya pengembang menggunakan sertifikat digital yang sudah tidak berlaku, *database* yang tidak terproteksi, dan pengabaian *standard practice* dalam pengembangan sistem yang diakses secara publik. Pengembang juga seharusnya dapat menerapkan proteksi keamanan pada perangkat keras, seperti *server* atau *hard disk*. Sejumlah kasus kebocoran data terjadi karena eksploitasi perangkat keras yang di dalamnya terdapat data pelanggan.

Di samping pemilik atau pengembang platform digital, penyelenggara jasa telekomunikasi juga memiliki peran besar dalam menjaga keamanan warga dari ancaman penipuan digital. Sebagian besar penggunaan perangkat digital memerlukan nomor telepon seluler untuk dapat mengakses berbagai layanan digital. Penting artinya bagi penyelenggara jasa telekomunikasi untuk meregistrasi kartu telepon pengguna yang sesuai dengan Nomor Induk Kependudukan dan Kartu Keluarga untuk mengetahui identitas pengguna (Samudra et al., 2018).

Kejelasan identitas ini dapat digunakan untuk menjangkau pengguna dan menjatuhkan hukuman jikalau terjadi penyalahgunaan. Di Indonesia aturannya sudah ada, tapi implementasinya belum memadai sehingga masih banyak penjualan kartu seluler yang sudah teregistrasi di lokapasar. Aturan yang lebih ketat juga bisa diberlakukan, seperti di negara Singapura, yang membatasi satu orang hanya dapat membeli kartu telepon dalam jumlah tertentu.

Penyelenggara jasa telekomunikasi atau operator seluler bertanggung jawab juga dalam menjaga keamanan data pribadi. Seperti diberitakan beberapa waktu yang lalu, ada indikasi data pribadi pelanggan perusahaan telekomunikasi atau operator seluler bocor. Perlindungan data pelanggan di perusahaan jasa telekomunikasi atau operator seluler telah diatur dalam Peraturan Menteri Kominfo (Permenkominfo) Nomor 12 Tahun 2016 tentang Registrasi Pelanggan Jasa Telekomunikasi. Peraturan ini menjelaskan bahwa penyelenggara wajib merahasikan data dan/atau identitas pelanggan. Perusahaan juga diwajibkan memiliki sertifikat ISO 27001 untuk menjaga keamanan informasi dalam mengelola data pelanggan.

Usulan pencegahan yang kedua terbanyak menyangkut kepastian hukum bagi penanganan kasus penipuan digital. Kajian hukum menunjukkan bahwa landasan hukum menyangkut penanganan kasus penipuan digital di Indonesia masih lemah (Zabidin, 2021).

Saat ini peraturan yang berlaku untuk menjerat kasus penipuan adalah Undang-Undang Hukum Pidana (KUHP) khususnya Bab XXV tentang perbuatan curang. Pasal 378 UU ini menjelaskan bahwa penipuan termasuk kejahatan yang berkaitan dengan hak milik dan hak-hak lain yang timbul dari hak milik.

Selain itu, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen juga berlaku mengatasi kasus penipuan terkait transaksi daring (Pasal 28 Ayat 1 UU ITE) dan transaksi konvensional (Pasal 10 UU Perlindungan Konsumsi dari kasus penipuan konvensional). Peraturan-peraturan ini tidak cukup memadai karena kasus penipuan digital sangat variatif, tidak sebatas transaksi elektronik atau kasus penipuan konvensional. Variasi kasus penipuan digital ini membawa tantangan pada proses pembuktian dan unsur-unsur yang dikategorikan sebagai perbuatan melanggar hukum pada sistem elektronik atau daring (Zabidin, 2021).

Beberapa tantangan yang menghambat aparat dalam penegakan hukum, antara lain yaitu pembuktian tindak pidana penipuan secara daring memerlukan infrastruktur dalam mendukung proses pembuktian dan ketersediaan sumber daya manusia yang terbatas dalam proses penegakan hukum (Zabidin, 2021).

Aparat penegak hukum juga dituntut teliti dalam menentukan pasal yang digunakan dalam penyelesaian perkara dan seharusnya dibekali kemampuan terkait teknologi yang memadai untuk mendukung proses penyidikan.

PENANGANAN PENIPUAN DIGITAL

Di samping pencegahan, survei juga menjajaki penanganan penipuan digital. Temuan survei menunjukkan bahwa penanganan penipuan digital yang menurut responden dapat mengatasi penipuan digital sebagai berikut:

70,5%
Pemberian hukuman setimpal bagi penipu dan kompensasi/ganti rugi bagi korban oleh penipu

65,8%
Ketersediaan sistem pelaporan yang memudahkan korban melapor

69,4%
Profesionalitas aparat dalam membantu korban

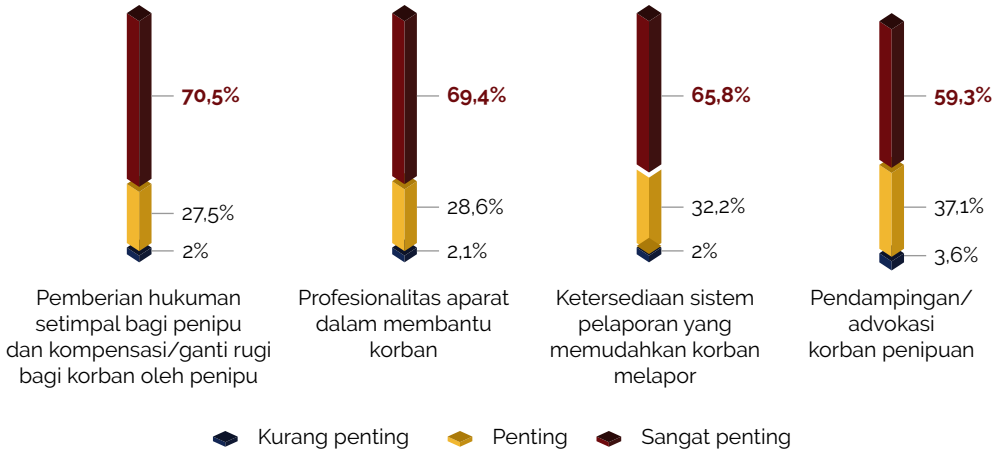
59,3%
Pendampingan/advokasi korban penipuan

Seperti pada program pencegahan penipuan digital, ada beberapa upaya penanganan penipuan digital yang dipandang sama penting oleh responden. Meski demikian, setelah dilakukan penggalian data lebih mendalam (dengan melihat porsi jawaban "sangat penting" yang diberikan responden), prioritas upaya program penanganan secara berurutan sebagai berikut:

1. Pemberian hukuman setimpal bagi penipu dan kompensasi/ganti rugi bagi korban oleh penipu (70,5%)
2. Profesionalitas aparat dalam membantu korban (69,4%)
3. Ketersediaan sistem pelaporan yang memudahkan korban melapor (65,8%)
4. Pendampingan/advokasi korban penipuan (59,3%)

Dengan demikian, prioritas utama program pencegahan adalah pemberian hukuman setimpal bagi penipuan dan kompensasi/ganti rugi bagi korban oleh penipu. Setelah itu, profesionalitas aparat dalam membantu korban, ketersediaan sistem pelaporan yang memudahkan korban melapor, dan pendampingan/advokasi korban penipuan.

Gambar 7.2. Program Menangani Penipuan Digital (N=1.700)



Banyaknya jawaban pada pemberian hukuman setimpal bagi penipu dan kompensasi/ganti rugi bagi korban oleh penipu mengindikasikan adanya kesan masyarakat bahwa sanksi yang diberikan kepada pelaku penipuan belum memuaskan. Weisse (2001) dalam artikelnya pernah mengungkapkan regulasi tanpa ancaman hukuman tidak akan efektif dalam menangani penipuan digital (Weisse, 2001).

Ketidakpuasan responden dalam penyelesaian kasus penipuan digital juga menyangkut pandangan responden terhadap aparat hukum. Sejumlah responden yang hadir dalam FGD mengungkapkan harapannya pada profesionalisme aparat dalam membantu korban mengatasi penipuan digital. Ada indikasi kuat kurang mempercayai kinerja aparat dalam penangangan kasus penipuan digital. Berikut beberapa kutipan hasil FGD yang menandai sikap masyarakat:

"Kalau melapor ke polisi dan tidak ada tindak lanjutnya, sama aja akan kecewa juga" **(MD, 27 tahun, FGD 9 April 2022).**

"Pelaporan ke pihak kepolisian boleh dikatakan tidak secepatnya mendapat respons…, jadi masyarakat merasa males akhirnya membuat laporan" **(IK, 58 tahun, FGD 9 April 2022)**

"Kepolisian pun tidak bisa berbuat banyak. Sampai polisi menyarankan untuk diikhlaskan saja. Bukan meremehkan institusi kepolisian. Tapi mungkin, mereka tidak bisa melacak atau mungkin tidak punya kekuatan untuk menangkap pelaku-pelaku penipuan digital" **(SB, 31 tahun, FGD 9 April 2022)**

Di samping itu, responden survei maupun peserta FGD sama-sama menghadapi kebingungan dalam melaporkan kasus penipuan digital. Oleh karena itu, mereka menyatakan perlunya ketersediaan sistem pelaporan yang memudahkan korban melapor. Bahkan dari hasil FGD muncul gagasan untuk membangun suatu sistem atau platform secara digital yang bersifat integratif untuk memudahkan warga melapor dan memudahkan petugas untuk menindaklanjuti kasus penipuan digital. Dalam hal ini responden mengusulkan agar UGM dan/atau perguruan tinggi lain bisa mengambil peran mengembangkan sistem atau platform tersebut.

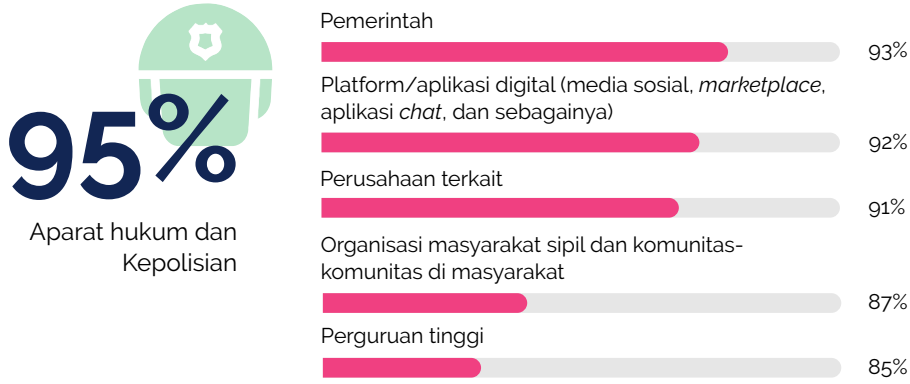
"Mungkin UGM bisa mengembangkan sistem pelaporan... Jadi ketika melapor tidak bingung lagi harus ke mana...masyarakat juga bisa mengecek, jenis-jenis penipuan itu seperti apa yang terjadi, biar kita lebih berhati-hati lagi" **(SB, 31 tahun, FGD 9 April 2022)**

PIHAK TERPERCAYA MEMBERIKAN INFORMASI PENCEGAHAN

Seiring naiknya tagar #PercumaLaporPolisi pada tahun 2021, kepolisian mendapatkan perhatian yang cukup tinggi di masyarakat Indonesia mengenai kualitas kinerjanya dalam memberantas tindak kriminal. Hasil survei Saiful Mujani Research and Consulting (SMRC) pada tahun 2021 mencatat tingkat kepercayaan publik terhadap lembaga penegak hukum tidak terlalu tinggi. Adapun untuk lembaga kepolisian mendapatkan 58% responden yang percaya dan 38% lainnya menyatakan tidak percaya.

Pihak yang paling dipercaya responden dalam memberikan informasi pencegahan dipegang oleh kepolisian (94,6%), sebagaimana tampak dalam grafik 7.3. Pihak pemerintah menempati posisi kedua sebagai pihak yang paling terpercaya dalam memberikan informasi pencegahan. Hasil olah data menunjukkan secara berturut-turut kepolisian 94,6%; pemerintah 92,9%; platform/aplikasi digital 92,2%; perusahaan terkait 91,4%; organisasi masyarakat sipil atau komunitas-komunitas di masyarakat 86,7%; dan perguruan tinggi 85,4%.

Gambar 7.3. Pihak Terpercaya Memberikan Informasi Pencegahan (N=1.700)



Bukan hanya di Indonesia, hasil survei Komisi Eropa di Uni Eropa (2020) terhadap masyarakat Uni Eropa juga menunjukkan hasil yang sama yaitu sebesar 41% responden tidak melaporkan pengalamannya terkait penipuan digital kepada otoritas dan sebesar 38% melaporkan kepada teman atau keluarga, namun tidak kepada otoritas.

Data ini menjadi pertimbangan bagi pihak terkait, khususnya kepolisian, yang menjadi ujung tombak dalam mencegah dan menangani penipuan digital, untuk lebih meningkatkan kinerjanya seperti dalam hal melayani kebutuhan masyarakat akan perlindungan hukum.

PIHAK YANG DIANGGAP RESPONDEN BERTANGGUNG JAWAB DALAM MENCEGAH DAN MENANGANI PENIPUAN DIGITAL

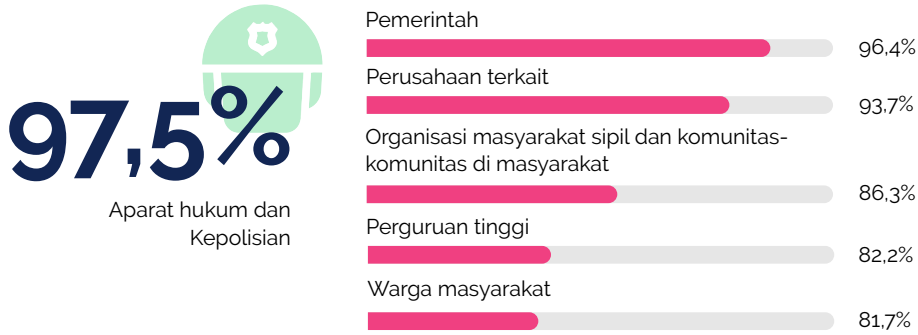
Pihak yang dinyatakan responden bertanggung jawab untuk mencegah dan menangani penipuan, secara berurutan sebagai berikut:

1. Kepolisian (97,5%)
2. Pemerintah (96,4%)
3. Perusahaan terkait (93,7%)
4. Organisasi masyarakat sipil atau komunitas-komunitas di masyarakat (86,3%)
5. Perguruan tinggi (82,2%)
6. Warga masyarakat (81,7%)

Seperti pada temuan sebelumnya (pihak yang dipercaya memberikan informasi pencegahan), responden juga menilai kepolisian juga sebagai pihak yang dianggap bertanggung jawab untuk mencegah dan menangani penipuan.

Sekali lagi temuan ini menegaskan pentingnya peningkatan kinerja institusi kepolisian dalam menangani penipuan digital.

Gambar 7.4. Pihak yang Bertanggung Jawab untuk Mencegah dan Menangani Penipuan Digital (N=1.700)



Kepolisian menempati posisi tertinggi sebagai pihak yang dipercaya dan dianggap bertanggung jawab oleh masyarakat untuk mencegah dan menangani penipuan digital. Namun, ironisnya, ketika responden menjadi korban, mereka cenderung tidak melapor kepada aparat hukum, kepolisian, dan lembaga otoritas terkait. Kepolisian menempati urutan nomor 5, diikuti oleh lembaga/otoritas terkait (OJK, Bappebti) dan lembaga pemerintah (kementerian). Seperti telah dijelaskan di depan, keengganan untuk melapor kasus penipuan digital ke aparat hukum dan kepolisian karena responden tidak puas dengan proses penanganan kasus.

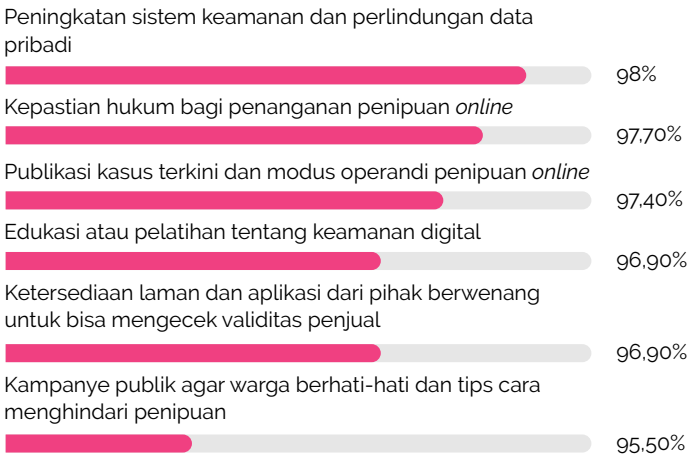
Studi yang dilakukan oleh Cross (2020) menunjukkan bahwa kepolisian memiliki keterbatasan kewenangan dan kemampuan dalam mengusut kasus-kasus penipuan digital. Regulasi yang ada dan bentuk penipuan digital yang bervariasi, bahkan melampaui batas-batas wilayah negara, memberikan tantangan bagi kepolisian. Studi ini merekomendasikan perubahan regulasi yang dapat memberi dukungan kepada kepolisian dalam penanganan kasus penipuan digital, peningkatan kapasitas sumber daya kepolisian dalam penyelidikan, dan pengadaan teknologi baru yang dapat membantu proses penyelidikan (Cross, 2020). Di samping itu, studi itu juga menyarankan perlunya komunikasi antara kepolisian dan warga, agar warga juga memahami keterbatasan kepolisian dalam mengungkap kasus penipuan digital.

REKOMENDASI PENCEGAHAN MENURUT KORBAN PENIPUAN DIGITAL

Seperti diuraikan di bagian awal, jenis penipuan digital sangat bervariasi. Penelitian ini mengidentifikasi 15 jenis penipuan digital. Secara umum, meski jenis penipuan digital bervariasi, rekomendasi pencegahan yang diutarakan oleh para korban penipuan digital cenderung sama. Dengan kata lain, apa pun jenis penipuan yang dialami korban, rekomendasi yang diberikan tidak jauh berbeda. Jika diurutkan, rekomendasi pencegahan penipuan digital yang disampaikan oleh para korban penipuan sebagai berikut:

1. Peningkatan sistem keamanan dan perlindungan data pribadi (98%)
2. Kepastian hukum bagi penanganan penipuan *online* (97,7%)
3. Publikasi kasus terkini dan modus operandi penipuan *online* (97,4%)
4. Edukasi atau pelatihan tentang keamanan digital (96,9%)
5. Ketersediaan laman dan aplikasi dari pihak berwenang untuk bisa mengecek validitas penjual (96,9%)
6. Kampanye publik agar warga berhati-hati dan tips cara menghindari penipuan (95,5%)

Gambar 7.5. Rekomendasi Pencegahan Menurut Korban Penipuan Digital (N=1.132)

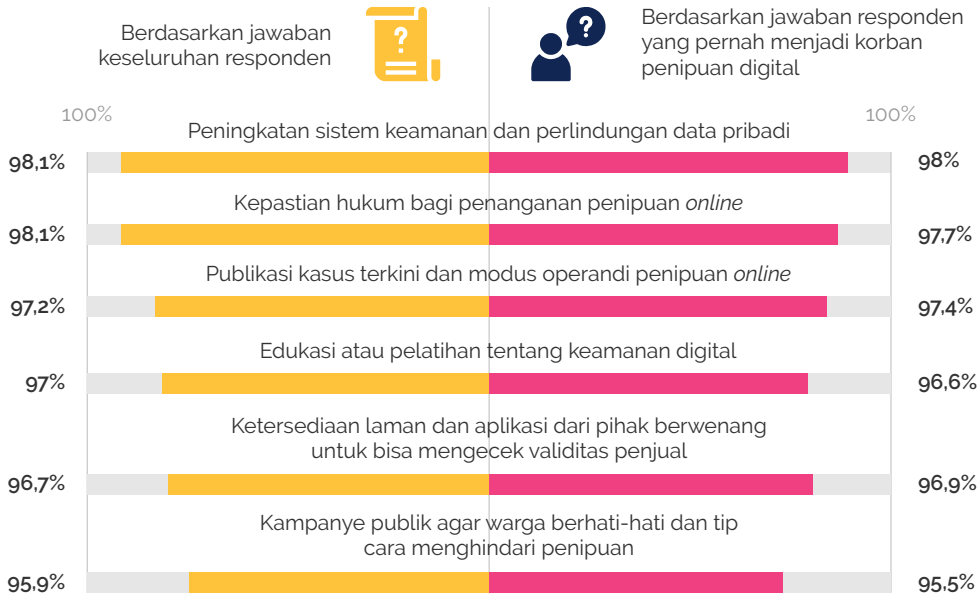


Rekomendasi pencegahan penipuan digital berdasarkan perspektif korban menarget masyarakat sendiri sebagai prioritas. Ini berkaitan dengan pengetahuan tentang kasus-kasus penipuan, termasuk modus-modusnya, dan kecakapan dalam keamanan digital. Kampanye publik agar warga berhati-hati dan tip cara menghindari penipuan dapat menjadi bagian dari pemberdayaan warga.

Rekomendasi selanjutnya berkenaan dengan fasilitasi pihak-pihak yang berwenang atau terkait, meliputi ketersediaan situs web dan aplikasi dari pihak berwenang untuk bisa mengecek validitas penjual, kepastian hukum bagi penanganan penipuan digital, dan peningkatan sistem keamanan dan perlindungan data pribadi.

Jika rekomendasi pencegahan ini dibuat perbandingan antara jawaban keseluruhan responden dan jawaban responden yang pernah menjadi korban penipuan digital, maka urutan rekomendasi menunjukkan perbedaan.

Gambar 7.6. Perbandingan Rekomendasi Pencegahan Penipuan Digital



Temuan ini menunjukkan, bagi korban penipuan digital, informasi tentang kasus-kasus penipuan terkini termasuk modus operandinya sangat penting untuk diketahui masyarakat. Semacam peringatan dini, informasi ini dapat meningkatkan kewaspadaan masyarakat. Rekomendasi berikutnya adalah edukasi dan pelatihan tentang keamanan digital. Rekomendasi ini mengarah pada *capacity building* agar warga dapat melindungi dirinya. Data ini menunjukkan kesadaran para korban bahwa ketahanan diri merupakan titik sentral yang dapat menyelamatkan seseorang dari kasus penipuan digital.

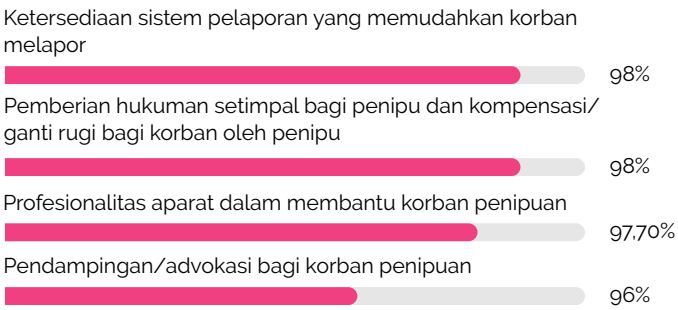
Jika rekomendasi para korban lebih cenderung mengarah pada 'peningkatan kapasitas diri' (berorientasi ke dalam), berbeda dengan rekomendasi yang disampaikan responden secara umum. Rekomendasi mereka lebih cenderung menuntut pihak lain untuk hadir melindungi warga agar terhindar dari penipuan digital (berorientasi ke luar).

REKOMENDASI PENANGANAN MENURUT KORBAN PENIPUAN DIGITAL

Rekomendasi penanganan penipuan digital yang diutarakan oleh para korban penipuan digital memiliki kecenderungan yang sama, meski jenis penipuan digital yang dialami bervariasi. Rekomendasi penanganan secara berurutan:

1. Ketersediaan sistem pelaporan yang memudahkan korban melapor (98%)
2. Pemberian hukuman setimpal bagi penipu dan kompensasi/ganti rugi bagi korban oleh penipu (98%)
3. Profesionalitas aparat dalam membantu korban (97,7%)
4. Pendampingan/advokasi korban penipuan (96%)

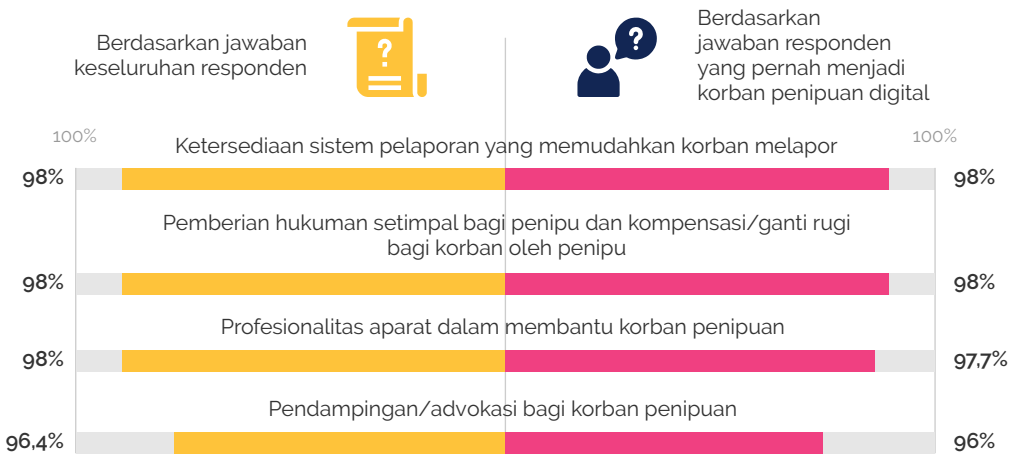
Gambar 7.7. Rekomendasi Penanganan Menurut Korban Penipuan Digital (N=1.132)



Profesionalitas aparat dalam membantu korban menjadi perhatian utama responden yang pernah menjadi korban penipuan. Meski ada pesimisme warga terhadap kinerja aparat, warga mengharapkan adanya upaya yang serius untuk meningkatkan profesionalitas dan kinerja aparat. Masyarakat pada dasarnya mengetahui bahwa mereka harus melapor ke aparat penegak hukum jika mengalami penipuan digital, namun mereka merasa sia-sia ketika laporannya tidak ditanggapi dan ditindaklanjuti secara memadai oleh kepolisian.

Jika dibandingkan dengan jawaban seluruh responden tentang rekomendasi penanganan ini, ada pergeseran pada rekomendasi pertama dan kedua. Jawaban seluruh responden, baik yang pernah menjadi korban penipuan maupun yang bukan korban, menempatkan jawaban "Pemberian hukuman setimpal bagi penipu dan kompensasi/ganti rugi bagi korban oleh penipu" sebagai prioritas pertama. Sementara itu, bagi yang pernah menjadi korban merekomendasikan "Profesionalitas aparat dalam membantu korban" sebagai yang utama. Perbedaan jawaban ini mengindikasikan betapa korban berharap banyak kepada aparat untuk dapat membantu penanganan kasus penipuan digital. Rekomendasi ini juga mengisyaratkan kembali adanya ketidakpuasan korban atas kinerja aparat.

Gambar 7.8. Perbandingan Rekomendasi Penanganan Penipuan Digital



Pencegahan penipuan digital memiliki bentuk yang bervariasi mulai dari peningkatan sistem keamanan dan perlindungan data pribadi, kepastian hukum bagi penanganan penipuan digital hingga kampanye publik agar warga berhati-hati dan tip-tip cara menghindari penipuan. Bagi para korban, rekomendasi pencegahan utama adalah publikasi kasus terkini dan modus operandi penipuan digital dan edukasi atau pelatihan tentang keamanan digital. Jika di-perbandingkan antara jawaban keseluruhan responden dan jawaban responden yang pernah menjadi korban penipuan digital, tampak ada perbedaan. Para responden yang menjadi korban lebih cenderung mengarah pada peningkatan kapasitas diri (berorientasi ke dalam), sementara responden secara umum kebanyakan cenderung menuntut pihak lain untuk hadir melindungi warga agar terhindar dari penipuan digital (berorientasi ke luar).

Temuan ini menunjukkan, adanya proses reflektif para korban dalam melihat kasus penipuan digital.

Dalam hal penanganan penipuan digital, riset ini menunjukkan pentingnya pemberian hukuman setimpal bagi penipu dan kompensasi/ganti rugi bagi korban oleh penipu, profesionalitas aparat dalam membantu korban dan ketersediaan sistem pelaporan yang memudahkan korban melapor. Tidak ada perbedaan menyolok antara jawaban keseluruhan responden dan jawaban responden yang pernah menjadi korban penipuan digital.

Temuan menarik lainnya, kepolisian merupakan pihak yang paling dipercaya dalam memberikan informasi pencegahan dan dianggap paling bertanggung jawab dalam penanganan kasus penipuan digital. Meski demikian, sebagian besar responden memilih untuk tidak melaporkan kasus penipuan yang dialaminya kepada kepolisian, karena tidak puas dengan kinerjanya dalam menanggapi dan menindaklanjuti laporan.

8

PENUTUP

PENUTUP

Buku yang disusun berdasakan riset nasional mengenai penipuan digital di Indonesia ini hadir bersamaan dengan meningkatnya kasus penipuan digital di Indonesia maupun pemberitaan mengenainya. Tak hanya jumlah korban penipuan digital yang meningkat, tapi juga medium dan modusnya yang juga semakin banyak. Hal ini menunjukkan tingginya kerentanan masyarakat terhadap penipuan digital sehingga alternatif solusi untuk mengatasinya perlu segera dilakukan secara bersama.

Agar bisa merekomendasikan kebijakan yang tepat, riset mengenai penipuan digital ini dilakukan dengan memetakan pesan, modus, medium, korban, kerugian, respons, dan rekomendasi. Riset yang melibatkan 1.700 responden dari 34 provinsi di Indonesia serta 31 informan ini tak hanya memetakan pesan, modus, medium, korban, dan kerugian penipuan digital, namun juga memetakan respons dan rekomendasi untuk mencegah dan menangani penipuan digital.

Bab penutup ini memberikan penekanan pada temuan utama riset ini namun juga kontribusinya secara akademis dan praktis terkait penipuan digital di Indonesia.

PEMETAAN PENIPUAN DIGITAL DI INDONESIA

Temuan riset ini menunjukkan bahwa pesan penipuan digital diterima oleh nyaris seluruh responden (98,3%) atau sejumlah 1.671 orang. Sedangkan yang menjadi korban sebanyak 66,6% responden (1.132 orang). Korban terbanyak berasal dari penipuan berkedok hadiah (36,9%) yang dilakukan melalui jaringan seluler (SMS dan telepon) sebagai medium yang paling banyak digunakan masyarakat Indonesia. Korban penipuan digital pun seolah bisa menimpa siapa saja, tanpa memandang usia maupun tingkat pendidikannya. Sementara kerugian yang menimpa korban pun sangat bervariasi baik secara material dan immaterial.

Meskipun modus penipuan digital sangat beragam sebagaimana temuan riset ini, terdapat sebuah pola tentang kelompok usia yang paling sering menjadi korban dan modus penipuan yang menyertai. Kecenderungan ini tampak dalam tabel di bawah ini yang menggambarkan persentase responden dari tiap generasi yang menjadi korban penipuan dan modus penipuan yang paling sering menimpa mereka.

Gambar 8.1. Generasi yang Paling Sering Menjadi Korban dan Modus yang Menyertai

Baby Boomer (1946-1964)

Persentase yang menjadi Korban
72,6%

Modus Penipuan yang Paling Sering Dialami
Penipuan berkedok hadiah

Generasi Z (1997-2012)

Persentase yang menjadi Korban
68,1%

Modus Penipuan yang Paling Sering Dialami
Pengiriman tautan berisi *malware*/virus

Generasi X (1965-1980)

Persentase yang menjadi Korban
67%

Modus Penipuan yang Paling Sering Dialami
Penipuan berkedok hadiah

Milenial (1981-1996)

Persentase yang menjadi Korban
62,8%

Modus Penipuan yang Paling Sering Dialami
Pengiriman tautan berisi *malware*/virus

REKOMENDASI PENCEGAHAN DAN PENANGANAN PENIPUAN DIGITAL DI INDONESIA

Ketika pemerintah Indonesia gencar mendorong pertumbuhan ekonomi digital dan menyuarakan besarnya potensi era digital bagi kehidupan, upaya memaksimalkan peluang itu perlu diimbangi dengan upaya yang sama besarnya untuk meminimalkan risiko yang muncul. Salah satu risiko itu adalah penipuan digital, sebuah tindak kejahatan yang juga menjadi tantangan besar di banyak negara lain karena kuantitas dan kualitasnya tumbuh seiring perkembangan teknologi.

Melihat cerita para korban penipuan digital dan mekanisme pelaporan serta penegakan hukum yang tersedia di Indonesia, upaya untuk meminimalkan risiko tersebut masih kurang optimal, bahkan bisa dikatakan tertinggal dengan upaya mitigasi yang dilakukan negara-negara lain. Karena itu, buku ini mencatat lima isu utama dan rekomendasi sebagai berikut:

Penertiban Nomer Seluler

Banyaknya nomor seluler aktif yang tidak terdaftar secara baik. Ini adalah persoalan besar mengingat penipuan melalui jaringan seluler (terutama SMS berhadiah) menjadi pesan atau modus penipuan yang paling banyak diterima responden sekaligus mencatat korban paling banyak. Berdasarkan cerita para korban penipuan dan pengalaman peneliti, pesan SMS penipuan berkedok hadiah menyerbu telepon seluler warga setiap hari, bahkan beberapa kali dalam sehari. Bagi sebagian warga, pesan-pesan itu dengan mudah diabaikan karena mereka sudah tahu itu adalah penipuan. Tapi bagi sebagian warga lain, yang jumlahnya banyak, pesan itu dipercaya dan berujung pada mereka menjadi korban.

Penjualan nomor seluler seakan-akan di luar kendali karena ada banyak toko di lokapasar yang menjual nomor seluler yang sudah "diregistrasi" sehingga pembeli bisa langsung memakainya tanpa melakukan registrasi sesuai aturan Kementerian Kominfo. Ini menjadi jalan yang sangat mudah bagi penipu memiliki banyak nomor seluler untuk melakukan penipuan.

Karena itu, Kementerian Kominfo, operator seluler, dan lokapasar perlu menertibkan penjualan nomor-nomor seluler untuk memastikan bahwa setiap pemilik nomor seluler sudah melakukan registrasi sesuai aturan yang berlaku sehingga identitas pemilik yang tercatat sesuai dengan pemakai yang sebenarnya. Di atas kertas, ini bukanlah hal yang mustahil, karena ada banyak negara lain yang bisa melakukannya, sehingga meminimalkan kasus penipuan melalui jaringan seluler.

Selain itu, operator seluler diharapkan tidak menjual kembali nomor seluler yang sudah tidak aktif. Ini dialami oleh peserta FGD, yang bercerita bahwa, setelah membeli nomor baru dan melakukan registrasi sesuai aturan Kementerian Kominfo, ia "diteror" oleh sejumlah pihak karena pemilik nomor yang lama terlibat utang dengan mereka.

Kepastian Hukum dalam Tindak Lanjut Laporan Penipuan Digital

Kejahatan siber menjadi ranah kepolisian dan kejaksaan, tapi yang pertama menghadapinya adalah kepolisian. Indonesia telah memiliki mekanisme pelaporan penipuan digital yang terpusat di Patrolisiber.id, yang dikelola oleh Direktorat Tindak Pidana Siber Bareskrim Polri. Namun, Direktorat Tindak Pidana Siber mengurus segala jenis kejahatan di ranah siber, seperti perjudian, pencemaran nama baik, ujaran kebencian, perdagangan manusia, pornografi anak, dan lain-lain sehingga kepolisian kewalahan untuk bisa menangani laporan penipuan digital sesuai harapan masyarakat.

Ini ditunjukkan oleh pengalaman para korban yang mengatakan bahwa mereka merasa diabaikan karena "kerugiannya kecil", "ada antrean korban lain yang kerugiannya jauh lebih banyak", dan "setelah lapor, tidak ada tindak lanjut" sehingga mereka harus ikhlas merelakan kerugian finansial yang dialami. Karena itu, untuk memberikan kepastian hukum yang lebih baik dalam penanganan penipuan digital yang kasusnya terus bertambah, divisi yang mengurusi penipuan digital perlu diperkuat secara infrastruktur dan sumber daya manusia yang bekerja intensif bersama otoritas lainnya.

Keseriusan otoritas di luar negeri untuk memininalkan risiko ini bisa dilihat pada contoh berikut. Di Inggris Raya, ada National Fraud Intelligence Bureau yang bersama Kepolisian London mengelola pusat pelaporan www.actionfraud.police. uk. Di Malaysia, ada pembagian tugas otoritas sesuai jenis penipuan, yaitu Bank Negara Malaysia sebagai regulator yang juga menyelidiki penipuan finansial, Malaysian Communications and Multimedia Commission (MCMC) yang menindaklanjuti kasus seperti penipuan melalui jaringan seluler, *phishing,* dan terkait pencurian data pribadi, lalu Ministry of Domestic Trade and Consumer Affairs untuk penipuan yang melibatkan hak konsumen seperti penipuan jual-beli di media sosial. Sementara itu, di Singapura pada awal 2022, untuk menanggapi tingginya aksi *phishing* melalui SMS yang menarget nasabah bank, serangkaian langkah bersama dirumuskan oleh para pemangku kepentingan (Monetary Authority of Singapore, Association of Banks in Singapore, Info-communications Media Development Authority, dan National Crime Prevention Council).

Perlindungan Data Pribadi dan Keamanan Siber

Dalam konteks yang lebih besar, beragam cerita penipuan yang disampaikan dalam laporan ini terkait dengan isu perlindungan data pribadi (seperti pemakaian NIK dan email dalam penipuan) dan keamanan siber (seperti peretasan server yang datanya dipakai untuk penipuan).

Saat laporan ini ditulis, Indonesia belum memiliki Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Keamanan dan Ketahanan Siber (UU KKS). RUU PDP masih belum selesai dibahas oleh pemerintah dan DPR RI. Sementara, RUU KKS bahkan masih belum dikirimkan ke DPR untuk dibahas. Keduanya adalah legislasi yang urgen untuk memayungi berbagai upaya mencegah dan menangani penipuan digital.

Jika UU PDP lebih berfokus pada mekanisme pengumpulan, penyimpanan, dan penggunaan data pribadi oleh pengendali data publik maupun swasta, UU KKS lebih berorientasi pada penciptaan ekosistem keamanan siber nasional, termasuk ancaman siber dari aktor luar negeri (Kustiasih, 2021).

UU KKS juga akan memperkuat peran Badan Siber dan Sandi Negara dalam menjalankan koordinasi menjaga keamanan ekosistem siber, termasuk menindak kejahatan siber yang penegakan hukumnya dilakukan oleh kepolisian.

UU PDP dan UU KKS bertujuan mewujudkan kepastian hukum dan rasa aman bagi warga. Keberadaan keduanya yang mengatur dengan rinci tugas, wewenang, dan fungsi lembaga swasta maupun publik akan menyediakan pondasi yang kuat bagi upaya meminimalkan risiko penipuan di era digital.

Sosialisasi dari Otoritas

Selaras dengan rekomendasi dari para responden, sosialisasi kepada warga tentang ancaman penipuan digital perlu terus dilakukan oleh berbagai otoritas, dari kepolisian hingga otoritas keuangan. Selain dilakukan secara terpisah, sosialisasi yang dilakukan secara terkoordinasi juga bisa menjadi cara untuk lebih meningkatkan jangkauan kepada masyarakat.

Sebagai salah satu contoh, Australia dan Selandia Baru pada 2015 membentuk Australasian Consumer Fraud Taskforce, yang kemudian berubah nama menjadi Scams Awareness Network, sebagai jejaring kerja beragam lembaga publik (misalnya kepolisian, komisi informasi, kementerian komunikasi, dan otoritas perlindungan konsumen) untuk menyebarkan informasi tentang penipuan digital secara rutin dan melakukan kampanye yang terkoordinasi kepada masyarakat.

Informasi dan data yang terpublikasikan dengan baik menjadi kunci terbangunnya pengetahuan dan kewaspadaan masyarakat dalam mencegah risiko penipuan digital. Publikasi berisi informasi terkini tentang jenis, medium, maupun modus penipuan digital terkini berikut panduan menghadapi dan mekanisme pelaporannya.

Kampanye Literasi Digital dari Non-otoritas

Riset ini dan berbagai riset sejenis di luar negeri menunjukkan, modus penipuan digital sangat beragam dan metodenya terus berkembang, sehingga program-program literasi digital kepada berbagai lapisan masyarakat perlu terus dilakukan untuk menanggapi dinamika tersebut.

Literasi digital adalah pondasi membangun pola pikir dan kecakapan menghadapi tantangan era digital. Dalam konteks penipuan digital, edukasi literasi digital diperlukan untuk mengaktifkan kewaspadaan masyarakat melalui pemahaman menyeluruh dari hulu-hilir tentang penipuan digital.

Berbeda dari sosialisasi dari otoritas, program ini perlu berangkat dari perspektif warga yang dianggap rentan terhadap penipuan digital sehingga sifatnya lebih tersegmentasi dan mendalam daripada sosialisasi.

DAFTAR PUSTAKA

Adikara, G. J., Kurnia, N., Adhrianti, L., Astuty, S., Wijayanto, X. A., Setyaningsih, F. D., Astuti, S. I. (2021). Modul aman bermedia digital. Direktorat Jenderal Aplikasi Informatika. https://drive.google.com/file/d/1iFJdhRpHSnEdDd5crUI3Es-IpQjqzYUi/view

Alfajri, I., Hidayat, A. R., Sarwindaningrum, I., & David, D. (2022, April 22). Jerat asmara penipu cinta berbingkai agama. Kompas.id. https://www.kompas.id/baca/investigasi/ 2022/04/21/jerat-asmara-penipu-cinta-berbingkai-agama

Aninsi, N. (2021, October 1). Game nomor 1 di Indonesia dengan pengunduh terbanyak di PlayStore. Katadata. https://katadata.co.id/safrezi/digital/61571f8cc46f2/game-nomor-1-di-indonesia-dengan-pengunduh-terbanyak-di-playstore

Arbi, I. A. (2021). Petaka pinjol yang sengsarakan warga, dipecat kantor, terjerat utang besar, hingga bunuh diri. Kompas.com. https://pemilu.kompas.com/read/2021/11/17/12232641/petaka-pinjol-yang-sengsarakan-warga-dipecat-kantor-terjerat-utang-besar

Arifin, M. (2022). Jadi korban penipuan online, Luna Maya ceritakan kronologinya. Merdeka.com. https://www.merdeka.com/jabar/jadi-korban-penipuan-online-luna-maya-ceritakan-kronologinya.html

Astuty, S. (2021). Memahami dan menghindari penipuan digital. In G.J. Adikara & N. Kurnia (Eds.), Modul aman bermedia digital (pp.86-115). Direktorat Jenderal Aplikasi Informatika.

Babbie, E. (2013). The practice of social research. 13th edition. Wadsworth Cengage Learning.

Badawi, E. M. H. (2021). Towards algorithmic identification of online scams [Doctoral dissertation, University of Ottawa]. uOttawa Theses.

Barasa, A. M. (2022, April 22). Penipuan seller Shopee melalui "live sale", barang diklaim original tapi ternyata palsu. Media Konsumen. https://mediakonsumen.com/2022/04/22/surat-pembaca/penipuan-seller-shopee-melalui-live-sale-barang-diklaim-original-tapi-ternyata-palsu

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. Psychology, Crime & Law, 20(3), 261-283. https://doi.org/10.1080/1068316X.2013.772180

Burhan, F. A. (2021, July 14). Akibat pandemi, pengaduan pinjaman online ilegal melonjak 80%. Katadata. https://katadata.co.id/intannirmala/digital/60ee9449b5a27/akibat-pandemi-pengaduan-pinjaman-online-ilegal-melonjak-80

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408. https://doi.org/10.1177/0004865814521224

Button, M., & Cross, C. (2017). Cyber frauds, scam and their victims. Routledge.

Canada. Competition Bureau Canada. (2012). The little black book of scams: Your guide to protection against fraud. https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/lbbs-web-2017-eng.pdf/$file/lbbs-web-2017-eng.pdf

CfDS. (2020). Kajian peningkatan kompetensi keamanan digital di Indonesia: Analisis fenomena penipuan dengan teknik rekayasa Sosial. CfDS.

Cross, C., Smith, R. G., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. Trends & issues in crime and criminal justice, 474. https://www.aic.gov.au/sites/default/files/2020-05/tandi474.pdf

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. Criminology & Criminal Justice, 20(3), 358-375. https://doi.org/10.1177/1748895819835910

Dam, T., Klausner, L. D., & Schrittwieser, S. (2020). Typosquatting for fun and profit: Cross-country analysis of pop-up scam. Journal of Cyber Security and Mobility. https://doi.org/10.13052/jcsm2245-1439.924

Department for Digital, Culture, Media & Sport, Home Office. (2022, March 8). Major law changes to protect people from scam adverts online. Gov.Uk. https://www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online

Dihni, V. A. (2021, October 7). Kerugian akibat kejahatan siber capai Rp 3,88 triliun, apa saja bentuknya?. Databoks. https://databoks.katadata.co.id/datapublish/2021/10/07/kerugian-akibat-kejahatan-siber-capai-rp-388-triliun-apa-saja-bentuknya

Eka, R. (2020, May 29). Bagaimana perusahaan digital antisipasi isu keamanan dan privasi data: Diskusi bersama AVP information security Blibli Ricky Setiadi. Daily Social. https://dailysocial.id/post/tips-keamanan-dan-privasi-data-ricky-setiadi

European Union. Directorate-General for Justice and Consumers. (2020). Survey on "scams and fraud experienced by consumers". Ipsos. https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

Fahillah, I. (2022). Muncul lagi! Investasi bodong diduga tipu 45 orang, kerugian Rp 20 miliar. Detik.com. https://finance.detik.com/fintech/d-6051650/muncul-lagi-investasi-bodong-diduga-tipu-45-orang-kerugian-rp-20-miliar

Federal Trade Commission Consumer Advice. (n.d.). How to spot, avoid, and report tech support scams. Federal Trade Commission Consumer Advice. https://consumer.ftc.gov/articles/how-spot-avoid-report-tech-support-scams

Federal Trade Commission Consumer Advice. (n.d.). How to recognize and report spam text messages. Federal Trade Commission Consumer Advice. https://consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages

Gatra, S. (2021, August 11). Fotonya disebar dengan narasi pelecehan, korban pinjol lapor polisi. Kompas.com. https://megapolitan.kompas.com/read/2021/08/11/08385661/ fotonya-disebar- dengan-narasi-pelecehan-korban-pinjol-lapor-polisi?page=all

GWI. (2022). GWI's flagship report on the latest trends in social media. GWI. https://www.gwi.com/reports/social

Hidayat, R. (2021, November 8). "Sudah Ikhlas": Banyaknya kasus penipuan daring tak diproses polisi. Tirto.id. https://tirto.id/sudah-ikhlas-banyaknya-kasus-penipuan-daring-tak-diproses-polisi-gk9r

Indonesia. Badan Pusat Statistik. (2020). Hasil sensus penduduk 2020. https://www.bps.go.id/pressrelease/2021/01/21/1854/hasil-sensus-penduduk-2020.html

Indonesia. Badan Pusat Statistik. (2020). Potret pendidikan Indonesia: Statistik pendidikan 2020. https://www.bps.go.id/publication/2020/11/27/347c85541c34edae54395a3/statistik-pendidikan-2020.html

Indonesia. Badan Pusat Statistik Repulik Indonesia. (2020). Jumlah penduduk menurut wilayah, klasifikasi generasi, dan jenis kelamin, di Indonesia. https://sensus.bps.go.id/topik/tabular/sp2020/85/175748/0

Inez. (2022, March 19). Apa itu tinder swindler? Viral video penangkapan James Daniel Sinaga tinder swindler Indonesia. Tribun Jateng. https://jateng.tribunnews.com/2022/03/19/apa-itu-tinder-swindler-viral-video-penangkapan-james-daniel-sinaga-tinder-swindler-indonesia

Jhaveri, A. (2015, July 15). Faking it — scammers' tricks to steal your heart and money. Federal Trade Commission Consumer Advice. https://consumer.ftc.gov/consumer-alerts/2015/07/faking-it-scammers-tricks-steal-your-heart-and-money

Judhita, C. (2015). Communication patterns in cybercrime: Love scams case. Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika, 6(2), 29-40. https://jurnal.kominfo.go.id/index.php/jppki/article/view/592

Juliati, S. (2022, March 14). Cerita kobran Indra Kenz: Rugi ratusan juta, terjerat utang pinjol hingga berat badan turun 12 Kg. Tribunnews. https://www.tribunnews.com/nasional/2022/03/14/cerita-korban-indra-kenz-rugi-ratusan-juta-terjerat-utang-pinjol-hingga-berat-badan-turun-12-kg?page=3

King, D. L., Billieux, J., Delfabbro, P., & Potenza, M. (2020). Problematic online gaming and the COVID-19 pandemic. Journal of Behavioral Addictions, 9(2), 184-186. https://doi.org/10.1556/2006.2020.00016

Kount. (n.d.) 5 online gaming fraud schemes that lose revenue, discourage players. Kount. https://kount.com/blog/effects-online-gaming-fraud-schemes/

Kumparan.com. (2021, October 26). Studi: Indonesia rentan penipuan lewat telepon. Kumparan.com. https://kumparan.com/kumparantech/studi-indonesia-rentan-penipuan-lewat-telepon-1wnHrBoW9Nt

Kurnia, N., Adikara, J.A, Widodo, Y, & Astuty, S. (2022). Jangan lengah, pastikan tidak ada celah kejahatan digital. In Amihardja, S., Kurnia, N., & Monggilo, Z. M. Z (Eds.), Lentera literasi digital Indonesia: Panduan literasi digital kaum muda Indonesia Timur (pp. 101-181). Penerbit Tiga Serenada.

Kustiasih, R. (2021, October 31). Peretasan sistem pemerintah berulang, RUU keamanan siber bisa jadi solusi. Kompas.id. https://www.kompas.id/baca/polhuk/2021/10/30/peretasan-sistem-pemerintah-berulang-ruu-keamanan-siber-bisa-jadi-solusi

Linggauni. (2022, April 26). Polda NTB telusuri dugaan penipuan penjualan minyak goreng di Medsos. IDN Times NTB. https://ntb.idntimes.com/news/ntb/linggauni/polda-ntb-telusuri-dugaan-penipuan-penjualan-minyak-goreng-di-medsos/3

Merdeka. (2021, December 1). Lapor ke Kemkominfo, situs penipuan catut nama Schneider Electric. Merdeka.com. https://www.merdeka.com/teknologi/lapor-ke-kemkominfo-situs-penipuan-catut-nama-schneider-electric.html

Nadiroh, I. (2021, October 29). Upaya penipuan mengatasnamakan Shopee, bisa tahu alamat saya secara detail. Media Konsumen. https://mediakonsumen.com/2021/10/29/surat-pembaca/upaya-penipuan-mengatasnamakan-shopee-bisa-tahu-alamat-saya-secara-detail

New Zealand Government Department of Internal Affairs. (n.d.). Online scams. New Zealand Government Department of Internal Affairs. https://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Spam-Online-scams

Okezone. (2021, October 18). Korban pinjol ilegal yang merasa terintimidasi bisa dapat bantuan hukum gratis, begini caranya. Okezone.com. https://nasional.okezone.com/read/2021/10/18/337/2488247/korban-pinjol-ilegal-yang-merasa-terintimidasi-bisa-dapat-bantuan-hukum-gratis-begini-caranya

Pahlevi, R. (2022, January 10). YLKI catat 535 aduan konsumen sepanjang 2021. Databoks. https://databoks.katadata.co.id/datapublish/2022/01/10/ylki-catat-535-aduan-konsumen-sepanjang-2021

Pinandhita, V. (2022, April 21). Korban 'Ghosting' dating apps bisa trauma dobel, rugi materi plus dihakimi. Detik Health. https://health.detik.com/berita-detikhealth/d-6043883/korban-ghosting-dating-apps-bisa-trauma-dobel-rugi-materi-plus-dihakimi/2

Prass, A. B. (2022, April 21). Ditangani Mabes Polri gadis Kudus korban penipuan Indra Kenz rugi Rp2,5 Miliar. Krjogja. https://www.krjogja.com/berita-lokal/jateng/pantura/ditangani-mabes-polri-gadis-kudus-korban-penipuan-indra-kenz-rugi-rp-25-miliar/

Puram, P. K., Kaparthi, M., & Rayaprolu, A. K. H. (2011). Online scams: Taking the fun out of internet. Indian Journal of Computer Science and Engineering (ICJSE), 2(4), 559-565. https://www.researchgate.net/publication/267218231_ONLINE_SCAMS_TAKING_THE_FUN_OUT_OF_THE_INTERNET

Pusparisa, Y. (2020, September 11). Ribuan penipuan online dilaporkan dalam lima tahun terakhir. Databoks. https://databoks.katadata.co.id/datapublish/2020/09/11/ribuan-penipuan-online-dilaporkan-tiap-tahun

Rahayu, D. N. H. (2022). Waspada romance scam: Penipuan yang 'memainkan' aspek psikologis korban menggunakan platform teknologi. The Conversation. https://theconversation.com/waspada-romance-scam-penipuan-yang-memainkan-aspek-psikologis-korban-menggunakan-platform-teknologi-180579

Rahmanto, T. Y. (2019). Penegakan hukum terhadap tindak pidana penipuan berbasis transaksi elektronik. Jurnal Penelitian Hukum De Jure, 19(1), 31-52. http://dx.doi.org/10.30641/dejure.2019.V19.31-52

Ravianto. (2022, January 15). Perempuan warga cianjur dilaporkan ke Polda Jabar, kasus investasi online yang diduga bodong. TribunJabar.id. https://jabar.tribunnews.com/2022/01/15/perempuan-warga-cianjur-dilaporkan-ke-polda-jabar-kasus-investasi-online-yang-diduga-bodong

Retnowati, Y. (2015). Love scammer: Komodifikasi cinta dan kesepian di dunia maya. Jurnal Komunikologi, 12 (2), 65-77.

Riyanto, G. (2021, October 18). Jumlah pengguna aplikasi marketplace Indonesia terbesar ketiga di dunia. Kompas.com. https://tekno.kompas.com/read/2021/10/18/14130097/jumlah-pengguna-aplikasi-marketplace-indonesia-terbesar-ketiga-di-dunia?page=all

Sahrul. (2022). Jadi korban penipuan arisan online, wanita di Tanjungpinang lapor polisi, alami kerugian belasan juta. Barometerrakyat.com. https://barometerrakyat.com/jadi-korban-penipuan-arisan-online-wanita-di-tanjungpinang-lapor-polisi-alami-kerugian-belasan-juta/

Samudra, A.H., Lisanawati, G., & Wijaya, N. (2018). Peran penyelenggara jasa telekomunikasi dalam upaya pencegahan dan penanggulangan tindak pidana penipuan online di kota Surabaya. Project Report Universitas Surabaya, Surabaya. http://repository.ubaya.ac.id/36422/1/LAPORAN%20PENELITIAN%20PERAN%20PENYELENGGARA%20JASA%20TELEKOMUNIKASI_FINAL.pdf

Smith, R. G. (2010). Identity theft and fraud. In Y. Jewkes, & M. Yar (Eds.), Handbook of internet crime (pp. 273–301). Willan.

Sulaeman, R. Y. (2022, March 2). Hampir menjadi korban penipuan, proses buka blokir Mandiri tak kunjung selesai. Media Konsumen. https://mediakonsumen.com/2022/03/02/surat-pembaca/hampir-menjadi-korban-penipuan-proses-buka-blokir-mandiri-tak-kunjung-selesai

Sulaiman. F. (2021, April 13). Waspada! Investasi ilegal kian marak di masa pandemi. Warta Ekonomi. https://www.wartaekonomi.co.id/read336765/waspada-investasi-ilegal-kian-marak-di-masa-pandemi

Wardani, A. S. (2022, January 10). 5 Modus penipuan online ini semakin marak terjadi. Liputan6. https://www.liputan6.com/tekno/read/4854695/5-modus-penipuan-online-ini-semakin-marak-terjadi

Weisse, K. (2001). Remedies for internet fraud: Consumers need all the help they can get. Loyola Consumer Law Review, 14(2): 205-225. https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1318&context=lclr

We Are Social & Kepios. (2022). Digital 2022 Indonesia. Data Reportal. https://datareportal.com/reports/digital-2022-indonesia

Whitty, T. M. (2017). Do you love me? Psychological characteristics of romance scam victims. Cyberpsychology, Behavior, and Social Networking, 21(2), 1-5. https://doi.org/10.1089/cyber.2016.0729

Zabidin, Z. (2021). Analisis penegakkan hukum tindak pidana penipuan online di Indonesia. Jurnal Spektrum Hukum, 18(2). http://dx.doi.org/10.35973/sh.v18i2.2722

Buku berjudul "Penipuan Digital di Indonesia: Modus, Medium, dan Rekomendasi" disusun berdasarkan riset nasional berjudul sama yang dilakukan pada bulan Februari hingga Juni tahun 2022. Riset ini diawali dari keprihatinan atas semakin meningkatnya jenis penipuan digital terjadi di Indonesia. Sebagai salah satu kejahatan siber yang paling banyak terjadi, penipuan digital banyak menimbulkan korban dan berdampak pada kerugian finansial maupun non-finansial.

Agar bisa merekomendasikan solusi yang bersifat kolaboratif untuk mencegah dan menangani penipuan digital di Indonesia, riset nasional ini memetakan berbagai jenis pesan, modus, medium, kerugian, respons, dan rekomendasi yang diusulkan korban dan target penipuan digital di Indonesia.

Riset ini dilakukan atas kerja sama Center for Digital Society (CfDS) Fisipol UGM, Program Magister Ilmu Komunikasi Fisipol UGM, dan Pemantau Regulasi dan Regulator Media yang didukung oleh WhatsApp. Sebanyak 1700 responden dari 34 provinsi di Indonesia terlibat dalam survei nasional ini. Selain itu, 31 informan yang merupakan korban penipuan digital juga menjadi informan riset ini baik sebelum penyusunan instrumen survei maupun setelah terselenggaranya survei.

Atas terselenggaranya riset ini, kami mengucapkan terima kasih kepada WhatsApp sebagai pendukung utama dari penelitian yang dijalankan dalam program riset nasional berjudul "Penipuan Digital di Indonesia: Modus, Medium, dan Rekomendasi".

PENIPUAN DIGITAL DI INDONESIA: MODUS, MEDIUM, DAN REKOMENDASI

ISBN 978-623-99942-3-5 (PDF)