

Perancangan Iklan Layanan Masyarakat Pencegahan Phising

Raihan Mandala Putra¹, Vicia Dwi Prakarti DB²

¹Desain Komunikasi Visual, Institut Seni Indonesia Padangpanjang

²Televisi dan Film, Institut Seni Indonesia Padangpanjang

¹rehancoc546@gmail.com, ²viciadb21@gmail.com

Abstrak

Maraknya kasus kejahatan siber berupa *phishing* digital masih menjadi ancaman serius dalam keamanan informasi di Indonesia, salah satunya dipengaruhi oleh rendahnya literasi digital dan kurangnya kewaspadaan masyarakat usia produktif (20–50 tahun) dalam menjaga kerahasiaan data pribadi digital. Perancangan ini bertujuan untuk menghasilkan media informasi berbasis audio visual berbentuk Iklan Layanan Masyarakat (ILM) sebagai sarana edukatif bagi masyarakat dewasa guna mencegah penipuan digital dan melindungi privasi data digital. Metode yang digunakan dalam perancangan ini meliputi pendekatan kualitatif melalui observasi daring terhadap pola penyebaran serangan siber serta wawancara mendalam dengan pihak Satuan Reserse Kriminal (Reskrim) Polres Padang Panjang. Hasil pengamatan menunjukkan bahwa celah psikologis seperti kondisi kelengahan saat bekerja, manipulasi identitas, serta minimnya verifikasi terhadap tautan maupun file aplikasi berbahaya (APK) menjadi faktor utama tingginya kerentanan korban. Media informasi ini dirancang dalam bentuk video edukasi dengan pendekatan naratif realistik, penggunaan gaya visual antarmuka digital (*user interface*), serta rekonstruksi adegan nyata sehari-hari agar lebih persuasif. Hasil perancangan menunjukkan bahwa media audio visual ini berpotensi efektif menjadi sarana pendukung edukasi untuk meningkatkan kesadaran dan mengubah perilaku masyarakat agar lebih waspada terhadap ancaman *phishing*.

Kata Kunci: *phishing*, iklan layanan masyarakat, media informasi, audio visual

PENDAHULUAN

Data pribadi digital merupakan informasi yang bersifat rahasia dan harus dijaga keamanannya karena memuat identitas penting pengguna, seperti nama, alamat, nomor telepon, alamat surat elektronik (email), kata sandi, kode OTP, hingga informasi rekening maupun kartu pembayaran. Data tersebut menjadi bagian dari sistem autentikasi berbagai layanan digital dan pada umumnya hanya dapat diakses oleh pemilik data, penyedia layanan, serta aparat penegak hukum dalam kepentingan penyidikan. Selain berfungsi sebagai identitas pengguna, data pribadi digital juga memiliki peran penting dalam mendukung perkembangan ekonomi digital melalui berbagai aktivitas transaksi elektronik yang semakin meningkat.

Perkembangan teknologi informasi telah mendorong masyarakat menggunakan berbagai layanan digital, seperti media sosial, e-commerce, layanan hiburan, hingga perbankan digital. Seiring meningkatnya penggunaan layanan tersebut, masyarakat perlu memiliki kesadaran untuk menjaga kerahasiaan data pribadi dengan tidak membagikan informasi penting, seperti kata sandi, kode OTP, maupun data identitas kepada pihak yang tidak berwenang. Kurangnya pemahaman mengenai keamanan digital berpotensi meningkatkan risiko penyalahgunaan data pribadi serta berbagai bentuk penipuan daring.

Menurut data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2024, tingkat penetrasi internet di Indonesia telah mencapai 79,5% dari total populasi nasional. Angka tersebut merupakan capaian tertinggi dalam beberapa tahun terakhir yang menunjukkan semakin luasnya akses masyarakat terhadap internet. Meskipun demikian, tingkat penetrasi internet masih menunjukkan ketimpangan antarwilayah. Pulau Jawa mencatat penetrasi tertinggi sebesar 83,64%, disusul Kalimantan sebesar 77,42% dan Sumatera sebesar 77,34%, sedangkan Bali dan Nusa Tenggara mencapai 71,80%, Maluku dan Papua sebesar 69,91%, serta Sulawesi menjadi wilayah dengan penetrasi terendah sebesar 68,35%.

Meningkatnya penetrasi internet memberikan berbagai manfaat bagi masyarakat dalam memperoleh informasi, pendidikan, komunikasi, maupun layanan publik. Namun, di sisi lain, perkembangan tersebut juga diikuti oleh meningkatnya ancaman kejahatan siber. Salah satu bentuk kejahatan siber yang paling sering terjadi adalah *phishing*, yaitu tindakan penipuan yang dilakukan dengan menyamar sebagai pihak terpercaya, seperti instansi pemerintah, perusahaan, maupun lembaga perbankan, untuk memperoleh data pribadi korban secara ilegal.

Phishing merupakan metode penipuan digital yang memanfaatkan situs web, pesan singkat, email, maupun aplikasi percakapan yang dibuat menyerupai layanan resmi. Pelaku mengirimkan tautan palsu yang tampak meyakinkan agar korban memberikan informasi sensitif, seperti nama lengkap, kata sandi, nomor rekening, nomor kartu kredit, maupun kode OTP. Informasi tersebut kemudian disalahgunakan untuk mengambil alih akun atau melakukan transaksi tanpa sepengetahuan pemilik data.

Data RRI (2024) menunjukkan bahwa jumlah pengguna media sosial di Indonesia mencapai 191 juta orang atau sekitar 73,7% dari populasi, dengan pengguna aktif sebanyak 167 juta orang atau 64,3% dari populasi. Platform yang paling banyak digunakan adalah YouTube (139 juta pengguna), Instagram (122 juta), Facebook (118 juta), WhatsApp (116 juta), dan TikTok (89 juta). Berdasarkan kelompok usia, pengguna media sosial didominasi oleh rentang usia 18–34 tahun sebesar 54,1%. Rata-rata masyarakat Indonesia menghabiskan waktu sekitar 3 jam 14 menit setiap hari untuk mengakses media sosial dengan aktivitas utama berupa berbagi foto atau video, berkomunikasi, mencari informasi, hiburan, serta berbelanja secara daring.

Kelompok usia 20–50 tahun menjadi salah satu kelompok yang paling rentan terhadap serangan phishing karena memiliki intensitas penggunaan internet yang tinggi untuk bekerja, berkomunikasi, bertransaksi, maupun berbelanja secara daring. Pada kelompok usia 20–40 tahun, aktivitas multitasking sering menyebabkan pengguna kurang teliti ketika menerima pesan atau tautan yang mencurigakan. Sementara itu, pada kelompok usia 40–50 tahun, tingkat literasi digital yang relatif lebih rendah menyebabkan sebagian pengguna masih mudah percaya terhadap modus penipuan yang mengatasnamakan pihak bank, keluarga, maupun instansi tertentu. Beberapa penelitian juga menunjukkan bahwa mayoritas korban phishing melalui aplikasi WhatsApp berada pada rentang usia produktif, sehingga kelompok usia tersebut menjadi sasaran utama pelaku kejahatan siber.

Meningkatnya aktivitas digital turut diikuti oleh meningkatnya jumlah kasus penipuan digital di Indonesia. Berdasarkan data Indonesia Anti Scam Centre (IASC) yang dipublikasikan melalui Viva.co.id, sejak mulai beroperasi pada 22 November 2024 hingga awal tahun 2025, IASC menerima 30.124 laporan penipuan transaksi keuangan digital. Sebanyak 49.095 rekening dilaporkan terindikasi terlibat dalam aktivitas penipuan dengan total kerugian korban mencapai Rp476,6 miliar. Dari jumlah tersebut, hanya sekitar 20,14% dana yang berhasil diblokir sebelum digunakan oleh pelaku, sedangkan sebagian besar dana korban tidak dapat diselamatkan.

Tingginya angka kasus tersebut menunjukkan bahwa masih rendahnya kesadaran masyarakat dalam memverifikasi informasi sebelum memberikan data pribadi. Banyak korban langsung mengikuti instruksi yang diberikan pelaku tanpa melakukan pengecekan terhadap nomor pengirim, alamat situs web, maupun keaslian layanan yang menghubungi mereka. Padahal, langkah sederhana seperti mengabaikan pesan dari nomor yang tidak dikenal, memverifikasi informasi melalui kanal resmi, serta tidak sembarangan mengklik tautan dapat mengurangi risiko menjadi korban phishing.

Kasus phishing juga masih terus terjadi di Indonesia. Berdasarkan pemberitaan Kompas TV (2025), Direktorat Siber Polda Metro Jaya berhasil mengungkap kasus penipuan digital yang dilakukan oleh seorang tersangka berinisial D (30) pada April 2025. Pelaku mengirimkan tautan phishing melalui aplikasi WhatsApp dengan modus menyamar sebagai petugas bank yang meminta korban melakukan klarifikasi transaksi. Korban diarahkan untuk mengakses tautan palsu dan mengisi data pribadi berupa nama lengkap, nomor rekening, hingga kode OTP. Data tersebut kemudian dimanfaatkan pelaku untuk mengambil alih akses rekening korban.

Melihat tingginya angka penggunaan internet sekaligus meningkatnya kasus phishing, diperlukan media edukasi yang mampu meningkatkan kesadaran masyarakat mengenai pentingnya menjaga keamanan data pribadi digital. Salah satu media yang dinilai efektif adalah media audio visual karena mampu menggabungkan unsur gambar bergerak, suara, teks, dan narasi sehingga informasi dapat disampaikan secara lebih jelas, menarik, dan mudah dipahami.

Melalui media audio visual, proses terjadinya phishing dapat disimulasikan secara nyata, mulai dari penerimaan pesan mencurigakan, tindakan mengakses tautan palsu, hingga dampak yang ditimbulkan akibat kebocoran data pribadi. Penyajian tersebut diharapkan mampu memberikan gambaran yang lebih konkret sehingga masyarakat dapat mengenali berbagai bentuk modus phishing sekaligus memahami langkah-langkah pencegahannya.

Pemilihan media audio visual juga disesuaikan dengan karakteristik target audiens berusia 20–50 tahun yang merupakan pengguna aktif internet dan media sosial. Media ini mampu menyampaikan alur peristiwa secara runtut melalui perpaduan unsur visual dan audio sehingga hubungan sebab akibat dari setiap tindakan dapat dipahami dengan lebih baik. Oleh karena itu, perancangan media informasi berbasis audio visual diharapkan dapat menjadi sarana edukasi yang efektif dalam meningkatkan literasi keamanan digital serta menumbuhkan kesadaran masyarakat untuk melindungi data pribadi sebagai upaya pencegahan terhadap tindak phishing.

METODE

1. Metode Pengumpulan Data

a. Observasi

Observasi pada penelitian ini dilakukan secara online dengan menelusuri berbagai pemberitaan nasional, media sosial, dan platform digital pada 12 Juni 2025. Pengamatan difokuskan pada berbagai kasus phishing yang terjadi melalui WhatsApp, SMS, email, media sosial, serta penyebaran tautan palsu dan file APK berbahaya. Hasil observasi menunjukkan bahwa masih banyak masyarakat yang belum memahami cara mengenali penipuan digital sehingga mudah memberikan data pribadi atau mengunduh file dari sumber yang tidak resmi. Rendahnya literasi digital dan kurangnya kesadaran terhadap keamanan siber menjadi faktor utama meningkatnya kasus phishing di Indonesia.

Berdasarkan hasil penelusuran, ditemukan bahwa pelaku phishing sering memanfaatkan rekayasa sosial dengan menyamar sebagai pihak terpercaya, seperti bank atau instansi pemerintah, untuk memperoleh data pribadi korban. Beberapa kasus juga menunjukkan bahwa file APK berbahaya yang menyerupai dokumen resmi dapat mencuri kode OTP, informasi akun, hingga mengakses layanan perbankan digital. Temuan ini menunjukkan bahwa masyarakat masih rentan terhadap penipuan digital, sehingga diperlukan media edukasi yang sederhana, menarik, dan mudah dipahami untuk meningkatkan kesadaran dalam menjaga keamanan data pribadi.



Gambar 1. Observasi secara online grup jual web phishing

b. Wawancara

Wawancara dilakukan dengan pihak Satuan Reserse Kriminal (Reskrim) Polres Padang Panjang yang menangani laporan masyarakat terkait kasus phishing. Berdasarkan keterangan narasumber, modus penipuan yang paling sering terjadi dilakukan melalui SMS, telepon, WhatsApp, serta media sosial seperti Facebook dan Instagram. Pelaku biasanya menyamar sebagai orang yang dikenal korban untuk membangun kepercayaan. Dalam salah satu kasus, pelaku mengaku sebagai teman korban menggunakan nomor yang berbeda, kemudian meminta bantuan dana dengan alasan tertentu hingga korban mentransfer uang sebesar Rp13.000.000.

Setelah melakukan konfirmasi langsung kepada orang yang identitasnya digunakan, korban mengetahui bahwa dirinya telah menjadi korban penipuan dan melaporkan kejadian tersebut ke Polres Padang Panjang. Menurut pihak kepolisian, kasus ini menunjukkan bahwa phishing memanfaatkan kepercayaan korban melalui manipulasi identitas dan komunikasi digital. Oleh karena itu, masyarakat perlu lebih waspada, selalu memverifikasi identitas pengirim, serta tidak mudah memberikan informasi pribadi atau melakukan transfer sebelum memastikan kebenaran informasi yang diterima.



Gambar 2. Foto bersama dengan narasumber Satuan Reserse Kriminal (Reskrim) Polres Padang Panjang setelah kegiatan wawancara

c. Studi Pustaka

Pengumpulan data pada penelitian ini juga dilakukan melalui studi pustaka dengan menelaah berbagai sumber referensi yang relevan, seperti buku, skripsi, jurnal ilmiah, serta artikel ilmiah yang membahas perancangan media informasi berbasis audio visual. Studi pustaka ini bertujuan untuk memperoleh landasan teori, konsep, serta referensi mengenai prinsip-prinsip perancangan media informasi, komunikasi visual, penyusunan alur cerita, teknik penyampaian pesan, dan strategi penyajian informasi melalui media audio visual. Selain itu, kajian terhadap berbagai penelitian terdahulu digunakan sebagai acuan dalam menentukan konsep perancangan, menganalisis kelebihan dan kekurangan media yang telah dibuat sebelumnya, serta menjadi dasar dalam merancang media informasi yang lebih efektif, komunikatif, dan sesuai dengan karakteristik target audiens.

2. Metode Analisis Data

a. Analisis Target Audiens

1) Geografis

Perancangan Media informasi ditargetkan untuk orang dewasa yang ada di Indonesia.

2) Demografis

Perancangan media pembelajaran ditargetkan kepada dewasa yang ada di Indonesia berusia 20 sampai 50 tahun, baik laki-laki maupun perempuan.

3) Psikografis

Target audiens adalah masyarakat dewasa berusia 20–50 tahun yang aktif menggunakan perangkat digital dalam kehidupan sehari-hari, namun masih memiliki tingkat kewaspadaan yang beragam terhadap ancaman phishing. Sebagian audiens cenderung mudah mempercayai informasi yang diterima melalui media digital, terutama apabila pesan tersebut mengatasnamakan instansi resmi, kerabat, atau pihak yang dianggap terpercaya. Audiens juga memiliki motivasi untuk menggunakan layanan digital secara aman dalam aktivitas komunikasi, transaksi, dan pekerjaan, tetapi belum seluruhnya memiliki pemahaman yang memadai mengenai pentingnya verifikasi informasi, perlindungan data pribadi, serta risiko keamanan siber. Oleh karena itu, media informasi dirancang untuk meningkatkan kesadaran, kewaspadaan, dan kepedulian terhadap pentingnya menjaga keamanan data pribadi.

4) Behavior

Target audiens merupakan pengguna aktif internet yang terbiasa menggunakan telepon pintar, media sosial, aplikasi perpesanan, serta layanan perbankan digital dalam aktivitas sehari-hari. Audiens memiliki kebiasaan membuka tautan, mengunduh file, menerima pesan dari nomor yang tidak dikenal, serta melakukan transaksi digital melalui berbagai platform. Sebagian masih jarang melakukan verifikasi terhadap keaslian tautan, identitas pengirim, maupun sumber aplikasi sebelum memberikan data pribadi atau melakukan tindakan tertentu. Kebiasaan tersebut menyebabkan audiens memiliki risiko yang lebih tinggi menjadi korban phishing sehingga diperlukan media informasi yang dapat mendorong perilaku digital yang lebih aman dan waspada.

b. Analiss 5W+1H

1) What

Permasalahan yang diangkat dalam perancangan ini adalah masih tingginya kasus penipuan digital dalam bentuk phishing yang menyebabkan kebocoran data pribadi, pencurian akun, hingga kerugian finansial. Rendahnya literasi keamanan digital menyebabkan banyak masyarakat belum mampu mengenali ciri-ciri phishing maupun membedakan informasi yang asli dan palsu.

2) Where

Permasalahan phishing terjadi di ruang digital, terutama melalui media komunikasi seperti WhatsApp, SMS, email, media sosial, serta situs web palsu yang menyerupai layanan resmi. Berdasarkan hasil observasi dan wawancara, kasus serupa juga ditemukan di wilayah hukum Polres Padang Panjang, meskipun fenomena ini terjadi secara luas di Indonesia.

3) When

Kasus phishing dapat terjadi kapan saja selama masyarakat melakukan aktivitas digital, seperti berkomunikasi, berbelanja daring, mengakses layanan perbankan digital, maupun menggunakan media sosial. Seiring meningkatnya penggunaan internet dan layanan digital, kasus phishing terus berkembang dengan berbagai modus baru.

4) Why

Phishing terjadi karena pelaku memanfaatkan rendahnya literasi digital masyarakat melalui teknik rekayasa sosial (*social engineering*). Pelaku menggunakan identitas palsu, tautan berbahaya, situs web tiruan, maupun file aplikasi berbahaya untuk memperoleh data pribadi korban. Kurangnya kebiasaan melakukan verifikasi terhadap sumber informasi juga menjadi faktor yang meningkatkan risiko terjadinya phishing.

5) Who

Sasaran utama phishing adalah masyarakat pengguna internet, khususnya orang dewasa berusia 20–50 tahun yang aktif menggunakan media sosial, aplikasi perpesanan, layanan perbankan digital, serta berbagai layanan berbasis internet. Kelompok ini memiliki aktivitas digital yang tinggi sehingga lebih berpotensi menjadi sasaran pelaku phishing apabila kurang memahami keamanan digital.

6) How

Permasalahan tersebut diatasi melalui perancangan media informasi berbentuk audio visual berupa video *live action* yang menyajikan simulasi kasus phishing berdasarkan situasi yang sering terjadi di kehidupan sehari-hari. Media ini dilengkapi dengan penjelasan mengenai ciri-ciri phishing, dampaknya terhadap keamanan data pribadi, serta langkah-langkah pencegahannya. Penyampaian informasi melalui visualisasi situasi nyata diharapkan dapat meningkatkan pemahaman, kewaspadaan, dan mendorong masyarakat untuk menerapkan perilaku digital yang lebih aman.

3. Konsep Verbal dan Visual

a. Konsep Verbal

Konsep verbal dalam perancangan Iklan Layanan Masyarakat tentang pencegahan phishing ini dirancang sebagai upaya meningkatkan kesadaran masyarakat terhadap pentingnya menjaga keamanan data pribadi di era digital. Melalui penyampaian pesan yang sederhana, komunikatif, dan mudah dipahami, media ini diharapkan mampu memberikan pemahaman mengenai bahaya phishing serta langkah-langkah pencegahannya.

Gaya bahasa yang digunakan adalah Bahasa Indonesia yang sederhana dan dekat dengan kehidupan masyarakat sehari-hari. Penyampaian pesan dilakukan melalui narasi yang bersifat persuasif dan edukatif agar audiens dapat memahami risiko yang ditimbulkan oleh phishing tanpa merasa digurui. Pesan utama yang ingin disampaikan adalah pentingnya bersikap waspada terhadap tautan mencurigakan, permintaan data pribadi, serta berbagai modus penipuan digital yang mengatasnamakan pihak terpercaya.

b. Konsep Visual

Konsep visual dalam perancangan Iklan Layanan Masyarakat ini menggunakan pendekatan visual realistis yang menggambarkan situasi yang sering dialami masyarakat dalam kehidupan sehari-hari. Visual dirancang dengan nuansa modern dan profesional untuk merepresentasikan lingkungan digital yang menjadi ruang terjadinya aktivitas phishing.

Warna yang digunakan didominasi oleh biru, abu-abu, putih, dan merah sebagai penanda peringatan atau bahaya. Pemilihan warna tersebut bertujuan untuk menciptakan kesan aman, terpercaya, sekaligus memberikan penekanan pada situasi yang berpotensi mengancam keamanan data pribadi. Pengambilan gambar menggunakan variasi sudut kamera seperti *eye level*, *close up*, dan *over shoulder* untuk memperkuat penyampaian emosi serta membangun keterlibatan audiens terhadap cerita yang disajikan.

Selain itu, pada bagian akhir video digunakan motion graphic sebagai media pendukung untuk menyampaikan informasi pencegahan phishing secara lebih ringkas dan mudah dipahami. Penggunaan ikon, ilustrasi digital, tipografi,

serta animasi sederhana diharapkan dapat memperkuat pesan edukatif yang disampaikan dan membantu audiens mengingat langkah-langkah pencegahan phishing dengan lebih baik.

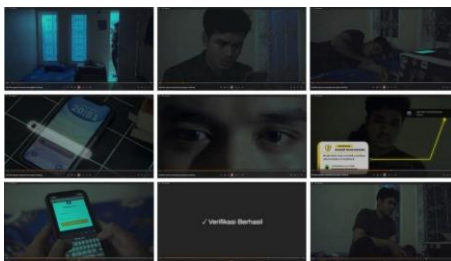
HASIL DAN PEMBAHASAN

1. Hasil Karya

a. Iklan Layanan Masyarakat

Video Iklan Layanan Masyarakat (ILM) Pencegahan Phishing merupakan media utama yang dirancang dalam format audio visual menggunakan teknik *live action* dan *motion graphic*. Video berdurasi 2 menit 47 detik ini dipublikasikan melalui YouTube dalam format MP4 dengan resolusi 4K (3840 × 2160 piksel) dan ditujukan kepada masyarakat berusia 20–50 tahun yang aktif menggunakan perangkat digital. Penyampaian pesan menggunakan pendekatan storytelling yang menggambarkan situasi sehari-hari ketika seseorang menerima pesan mencurigakan hingga menjadi korban phishing. *Motion graphic* digunakan untuk memperjelas ciri-ciri phishing, bentuk manipulasi pelaku, serta langkah-langkah pencegahannya sehingga informasi lebih mudah dipahami.

Alur video terdiri atas tiga bagian utama, yaitu pengenalan tokoh dan situasi, munculnya ancaman melalui pesan dari nomor tidak dikenal, serta puncak konflik ketika tokoh mengakses tautan palsu dan memberikan data pribadi. Penyajian visual menerapkan prinsip kesederhanaan, keterpaduan, penekanan, dan keseimbangan melalui penggunaan warna, tipografi, komposisi, serta variasi pengambilan gambar seperti *Wide Shot*, *Medium Shot*, *Close-Up*, dan *Extreme Close-Up*. Kombinasi unsur visual, audio, dan *motion graphic* tersebut diharapkan mampu menyampaikan pesan secara efektif, meningkatkan kesadaran masyarakat terhadap bahaya phishing, serta mendorong perilaku yang lebih bijak dalam menjaga keamanan data pribadi.



Gambar 3. Iklan Layanan Masyarakat

Tabel 1. Analisis Sinematografi Iklan Layanan Masyarakat Pencegahan Phishing

Scene	Waktu	Jenis Shot	Transisi	Deskripsi Visual	Fungsi
1	00:00–00:01	<i>Blank Screen</i>	<i>Fade In</i>	Layar hitam sebelum cerita dimulai.	Memberikan jeda visual sekaligus membuka alur cerita.
	00:01–00:04	<i>Wide Shot / Hard Cut Medium Long Shot</i>		Rian memasuki kamar kos setelah beraktivitas.	Memperkenalkan tokoh utama dan lingkungan cerita.
	00:04–00:06	<i>Insert Shot / Hard Cut Extreme Close-Up</i>		ID Card bertuliskan 'Rian Saputra' di atas meja.	Menegaskan identitas tokoh utama.
2	00:06–00:07	<i>Medium Shot</i>	<i>Hard Cut</i>	Rian duduk di tepi kasur.	Menunjukkan kondisi lelah setelah beraktivitas.
	00:07–00:13	<i>Extreme Close-Up</i>	<i>Hard Cut</i>	Layar telepon genggam dipenuhi notifikasi.	Memperlihatkan awal gangguan digital.
	00:13–00:19	<i>Medium Shot</i>	<i>Hard Cut</i>	Rian berbaring kemudian mengambil telepon genggam.	Menunjukkan rasa penasaran tokoh.
	00:19–00:24	<i>Close-Up</i>	<i>Hard Cut</i>	Pesan 'Capek ya? Jangan lupa istirahat'.	Menampilkan manipulasi psikologis awal.
	00:24–00:28	<i>Medium Long Shot</i>	<i>Hard Cut</i>	Rian menggantung jaket lalu kembali ke kasur.	Memberikan jeda sebelum konflik meningkat.
3	00:28–00:30	<i>Medium Shot</i>	<i>Hard Cut</i>	Rian bersiap tidur.	Menjadi transisi menuju konflik utama.

	00:30–00:36 <i>Close-Up</i>	<i>Hard Cut</i>	Pop-up 'Verifikasi Lanjutan' muncul di layar.	Memperlihatkan awal serangan phishing.
	00:36–00:53 <i>Medium Shot & Close-Up</i>	<i>Hard Cut</i>	Rian terbangun dan memperhatikan layar ponsel.	Membangun ketegangan.
	00:53–01:00 <i>Extreme Close-Up</i>	<i>Hard Cut</i>	Pesan intimidatif 'Kamu kelihatan pucat'.	Memberikan tekanan psikologis.
	01:00–01:14 <i>Medium Shot & Close-Up</i>	<i>Hard Cut</i>	Rian melihat ke seluruh ruangan.	Menggambarkan rasa paranoia korban.
	01:14–01:19 <i>Over the Shoulder</i>	<i>Hard Cut</i>	Bayangan mata tokoh terlihat melalui cermin.	Memperkuat nuansa thriller.
	01:19–01:36 <i>Medium Shot & Close-Up</i>	<i>Hard Cut</i>	<i>Chat phishing</i> disertai <i>overlay</i> edukasi.	Menjelaskan ciri nomor tidak dikenal.
	01:36–01:58 <i>Insert Shot / POV</i>	<i>Hard Cut</i>	Korban mengisi data pada website palsu.	Menunjukkan proses korban tertipu.
	01:58–02:05 <i>Full Screen Graphic</i>	<i>Hard Cut</i>	<i>Loading</i> hingga muncul 'Verifikasi Berhasil'.	Menandakan data korban berhasil dicuri.
	02:05–02:13 <i>Medium Shot</i>	<i>Fade Out</i>	Rian terdiam menyadari dirinya tertipu.	Menutup konflik sebelum edukasi.
4	02:14–02:34 <i>Motion Graphic</i>	<i>Fade In+ Slide</i>	Animasi simulasi layar ponsel dan browser.	Memberikan edukasi pencegahan phishing.
	02:34–02:39 <i>Static Typography</i>	<i>Hard Cut</i>	Tulisan 'Waspada phishing. Berpikir sebelum mengklik.'	Menegaskan pesan utama video.
	02:39–02:47 <i>Static Graphic</i>	<i>Hard Cut → Fade Out</i>	Logo institusi dan kredit kreator.	Menutup video serta menampilkan identitas karya.

b. Poster

Poster *feed* Instagram dirancang sebagai media pendukung yang terdiri atas sembilan *feed* edukatif dengan penyampaian informasi secara bertahap. *Feed* 1–3 berfungsi sebagai pembuka kampanye melalui visual *password*, kode OTP, dan judul "SEBELUM KLIK" untuk membangun kesadaran akan pentingnya menjaga data pribadi. *Feed* 4 menjelaskan pengertian dan proses terjadinya phishing, sedangkan *feed* 5 memaparkan ciri-ciri phishing, seperti nomor tidak dikenal, tautan mencurigakan, dan permintaan data pribadi. *Feed* 6 membahas dampak phishing, mulai dari pencurian data hingga pembobolan rekening, sementara *feed* 7 memberikan panduan mengenali website palsu melalui pemeriksaan alamat situs dan keamanan domain. *Feed* 8 mengingatkan pentingnya menjaga kerahasiaan *password* dan kode OTP, sedangkan *feed* 9 menutup rangkaian edukasi dengan langkah-langkah pencegahan phishing, seperti memverifikasi identitas pengirim, tidak sembarangan mengklik tautan, serta mengaktifkan fitur keamanan akun. Keseluruhan poster menggunakan warna biru sebagai identitas visual, dipadukan dengan ilustrasi, ikon, infografis, dan tipografi yang sederhana agar informasi mudah dipahami serta menarik bagi pengguna media sosial.





Gambar 4. Poster

c. Banner

Banner dirancang sebagai media pendukung edukasi yang terdiri atas dua seri dengan penyampaian informasi yang saling melengkapi. Banner pertama berisi pengertian phishing, cara kerja phishing, serta ciri-ciri umum yang perlu dikenali masyarakat melalui kombinasi infografis, ilustrasi, dan ikon digital. Sementara itu, banner kedua berfokus pada contoh pesan phishing dan langkah-langkah yang perlu dilakukan sebelum mengklik tautan, seperti memeriksa identitas pengirim, memastikan alamat situs, menghindari pesan yang bersifat mendesak, serta tidak memberikan data pribadi. Kedua banner menggunakan dominasi warna biru tua dengan aksen merah dan kuning untuk mempertegas informasi penting, serta tipografi *sans serif* yang mudah dibaca. Tata letak informasi disusun secara vertikal agar alur materi dapat diikuti dengan jelas, sehingga banner mampu menyampaikan edukasi mengenai phishing sekaligus meningkatkan kewaspadaan masyarakat dalam menjaga keamanan data pribadi saat beraktivitas di dunia digital.



Gambar 5. Banner

d. Zine

Zine dirancang sebagai media edukasi yang menyajikan informasi mengenai phishing secara ringkas, menarik, dan mudah dipahami. Sampul depan menampilkan judul "Waspada Phishing" dan "Berpikir Sebelum Mengklik" yang dipadukan dengan ilustrasi telepon genggam, halaman *login*, serta ikon peringatan untuk menggambarkan ancaman phishing, sedangkan sampul belakang memuat slogan "Lindungi Diri, Lindungi Data Pribadi" sebagai penegasan pesan utama. Isi *zine* disusun secara bertahap, dimulai dari penjelasan tentang pengertian dan cara kerja phishing, ciri-ciri phishing, contoh pesan palsu, serta langkah-langkah yang perlu dilakukan sebelum mengklik tautan. Selanjutnya, pembaca diberikan informasi mengenai data pribadi yang harus dijaga kerahasiaannya, seperti *password*, PIN, kode OTP, dan data perbankan, serta panduan yang harus dilakukan apabila terlanjur menjadi korban phishing. Keseluruhan *zine* menggunakan dominasi warna biru tua dengan aksen merah dan kuning, dipadukan dengan ilustrasi, ikon, dan tata letak yang sederhana sehingga informasi mudah dipahami serta mampu meningkatkan kesadaran masyarakat dalam menjaga keamanan data pribadi di ruang digital.



Gambar 6. Zine

KESIMPULAN

Perancangan skripsi berjudul “Perancangan Iklan Layanan Masyarakat Tentang Pencegahan Phishing Melalui Media Video Edukasi” menghasilkan media edukasi berbasis audio visual yang ditujukan kepada masyarakat berusia 20–50 tahun sebagai upaya meningkatkan kesadaran terhadap bahaya phishing. Perancangan ini didasarkan pada hasil observasi daring, studi pustaka, dan wawancara dengan pihak Reserse Kriminal Polres Padang Panjang yang menunjukkan bahwa rendahnya literasi digital, kurangnya kewaspadaan terhadap pesan mencurigakan, serta minimnya pemahaman mengenai ciri-ciri phishing menjadi penyebab utama meningkatnya kasus penipuan digital. Media utama berupa video Iklan Layanan Masyarakat menggunakan pendekatan storytelling untuk menggambarkan proses terjadinya phishing secara realistis, serta didukung oleh media pendukung berupa konten Instagram, video *reels*/TikTok, poster, banner, dan *zine* yang dirancang dengan identitas visual yang konsisten agar pesan edukasi dapat disampaikan secara sederhana, komunikatif, dan mudah dipahami.

Melalui perancangan ini diharapkan masyarakat dapat lebih bijak dalam menggunakan teknologi digital dengan selalu memverifikasi informasi, berhati-hati terhadap tautan atau file dari sumber yang tidak dikenal, serta menjaga kerahasiaan data pribadi. Selain itu, karya ini diharapkan dapat menjadi referensi bagi mahasiswa dan peneliti dalam mengembangkan media edukasi mengenai keamanan digital dengan pendekatan yang lebih inovatif. Pengembangan selanjutnya juga dapat memperluas pembahasan pada berbagai ancaman siber lainnya serta melibatkan kerja sama dengan institusi pendidikan, pemerintah, aparat penegak hukum, dan komunitas digital agar penyebaran informasi dapat menjangkau masyarakat secara lebih luas dan efektif.

UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas rahmat dan karunia-Nya sehingga karya skripsi berjudul “Perancangan Iklan Layanan Masyarakat Tentang Pencegahan Phishing Melalui Media Video Edukasi” dapat diselesaikan dengan baik. Dalam proses perancangan dan penyusunan karya ini, penulis memperoleh banyak dukungan, bantuan, serta arahan dari berbagai pihak. Penulis mengucapkan terima kasih kepada dosen pembimbing yang telah memberikan bimbingan, masukan, dan arahan selama proses penelitian hingga perancangan karya ini selesai. Terima kasih juga disampaikan kepada pihak Satuan Reserse Kriminal (Reskrim) Polres Padang Panjang yang telah bersedia memberikan informasi dan wawasan terkait kasus phishing sebagai data pendukung dalam penelitian ini. Ucapan terima kasih juga penulis sampaikan kepada seluruh dosen dan civitas akademika Program Studi Desain Komunikasi Visual yang telah memberikan ilmu, pengalaman, serta dukungan selama masa perkuliahan. Tidak lupa, penulis mengucapkan terima kasih kepada keluarga, teman-teman, serta semua pihak yang telah memberikan doa, motivasi, dan bantuan dalam proses penyelesaian karya ini. Semoga karya perancangan ini dapat memberikan manfaat bagi masyarakat dalam meningkatkan kesadaran terhadap keamanan data pribadi dan menjadi kontribusi dalam upaya edukasi mengenai pencegahan kejahatan digital, khususnya phishing.

DAFTAR PUSTAKA

- APJII. (2024). Jumlah pengguna internet Indonesia tembus 221 juta orang. <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>
- Ardan, F. (2021). Pengertian, jenis-jenis, serta fungsi media. Media Indonesia. <https://mediaindonesia.com/humaniora/451206/pengertian-jenis-jenis-serta-fungsi-media>
- Betancourt, M. (2013). The history of motion graphics: From avant-garde to industry in the United States. Wildside Press.
- CNN Indonesia. (2023). Bareskrim tangkap 13 tersangka penipuan link phishing, korban 493 orang. <https://www.cnnindonesia.com/nasional/20230120102615-12-902941/bareskrim-tangkap-13-tersangka-penipuan-link-phising-korban-493-orang>.
- Elvaretta, V., & Ahmad, A. (2021). Perancangan film pendek yang berjudul "Ask Myself".
- Galihleo, M. G., Umriyah, N. A., Nugroho, N. A., Farez, R. A., & Suryasuciramdhan, A. (2025). Iklan layanan masyarakat dalam mempengaruhi opini publik. Dialogika: Jurnal Penelitian Komunikasi dan Sosialisasi, 1(3).
- Gallagher, R., & Paldy, A. (2007). Exploring motion graphics. Thomson Delmar Learning.
- Hadi, A. P. (2022). Definisi, sejarah, dan prinsip dalam motion graphic. STEKOM. <https://komputer-grafis-d3.stekom.ac.id/informasi/baca/DEFINISI-SEJARAH-DAN-PRINSIP-DALAM-MOTION-GRAPHIC/a837951a23f133a46c5f3d5d7c1ed6561d083e24>.
- <https://ilmukomunikasi.uma.ac.id/2022/02/12/media-online/>
- Javandalasta, P. (2021). Storyboard untuk produksi film dan multimedia. IN Media.

- Kompas TV. (2024). Pelaku penipuan dengan link phishing via WhatsApp <https://www.kompas.tv/regional/592303/pelaku-penipuan-dengan-link-phising-via-whatsapp-ditangkap-perhatikan-modusnya>.
- Kompas.com. (2023). Pengakuan pembobol rekening Rp2,3 M lewat file APK di Palembang. <https://regional.kompas.com/read/2023/09/27/193524478/pengakuan-pembobol-rekening-rp-23-m-lewat-file-apk-di-palembang>.
- Mascelli, J. V. (1998). The five C's of cinematography: Motion picture filming techniques. Silman-James Press.
- Nugroho, H., Ihsan, M. N., Haryoko, A., Ma'arif, F., & Alifah, F. (2023). Edukasi keamanan digital untuk meningkatkan kewaspadaan masyarakat terhadap link phishing. *Alahyan Jurnal Pengabdian Masyarakat Multidisiplin (ECOS-PRENEURS)*, 1(2), 104–111.
- Nurholis, M. (2012). Pengertian media informasi. <https://holiskakashi.blogspot.com/2012/11/pengertian-media-informasi.html>.
- Putra, R. W. (2021). Pengantar desain komunikasi visual dalam penerapan.
- Putri, V. K. M. (2021). Media cetak: Pengertian dan jenisnya. Kompas.com. <https://www.kompas.com/skola/read/2021/12/06/103349769/media-cetak-pengertian-dan-jenisnya>
- RRI. (2024). Ini data statistik penggunaan media sosial masyarakat Indonesia tahun 2024. <https://www.rri.co.id/iptek/721570/ini-data-statistik-penggunaan-media-sosial-masyarakat-indonesia-tahun-2024>.
- Rustan, S. (2011). Font & tipografi. Gramedia Pustaka Utama.
- Rustan, S. (2017). Layout: Dasar & penerapannya. Gramedia Pustaka Utama.
- Ryan. (2022). Media online. Ilmu Komunikasi Universitas Medan Area.
- Zabarrekha Assidiq, M. (2023). Apa itu desain grafis? Berikut kemampuan atau skill desain grafis yang wajib kamu kuasai. Telkom University. <https://telkomuniversity.ac.id/apa-itu-desain-grafis-berikut-kemampuan-atau-skill-desain-grafis-yang-wajib-kamu-kuasai>.