DIVAGATRA
E-ISSN 2776-656X
https://ojs.unikom.ac.id/index.php/divagatra
Jurnal Penelitian Mahasiswa Desain
Vol. 03 No. 02 (Oktober 2023) Hal. 204-221

Perancangan Animasi sebagai Media Edukasi Kesadaran Masyarakat terhadap Kasus Penipuan File APK

Nikkolas Fassa[1], Dewi Isma Aryani[2], Elizabeth Wianto[3]
[1,2,3]*Desain Komunikasi Visual, Fakultas Seni Rupa dan Desain, Universitas Kristen Maranatha, Bandung*
Email: [1]nikkolas223@gmail.com, [2]dewi.ia@art.maranatha.edu, [3]elizabeth.wianto@art.maranatha.edu

Abstrak: Kejahatan siber merupakan suatu bentuk kejahatan baru yang berkaitan dengan jaringan komunikasi dan teknologi seperti internet, komputer, dan lain-lain. Pada bulan Desember tahun 2022 muncul sebuah bentuk kejahatan siber baru dengan cara menggunakan file APK untuk memperdayai korban-korbannya. Pelaku kejahatan siber menipu korban dengan cara berpura-pura menjadi orang penting seperti petugas PLN, aparat kepolisian, kurir paket, saudara yang mengirimkan surat undangan, dan lain sebagainya. Pelaku kejahatan siber tersebut memanfaatkan fitur pesan pribadi lalu mengirimkan pesan yang bersifat persuasif agar korban menginstal aplikasi khusus yang nantinya dapat mencuri data-data pribadi bahkan dapat mengambil saldo tabungan dari rekening korban. Penelitian ini bertujuan untuk mengedukasi masyarakat, khususnya berusia 40-60 tahun yang rentan terhadap kejahatan siber. Hasil pengumpulan dan analisis data menggunakan studi pustaka, survei, dan wawancara berdasarkan testimoni responden terpilih. Adapun visualisasi desain yang digunakan berupa ilustrasi *flat vector* sederhana supaya mudah dipahami oleh target. Oleh karena itu,dapat disimpulkan bahwa animasi edukatif ini dapat dijadikan media edukasi tentang berbagai bentuk kejahatan siber untuk meningkatkan kewaspadaan masyarakat pada era digital ini.

Kata kunci: *file* APK, kejahatan siber, kesadaran siber, kasus penipuan *online*.

Abstract: *Cybercrime is a brand-new category of crime that involves computer and other technology-based communication networks. In December 2022, a brand-new type of cybercrime surfaced that conned its victims by exploiting APK files. Cybercriminals trick their victims by posing as important individuals as PLN officers, police officers, parcel couriers, family members who send invitation letters, and so forth. When a victim installs a specific program, cybercriminals can steal personal information and even withdraw savings balances from the victim's account by using the private message feature and convincing messages. This study seeks to inform the general population, particularly at-risk demographics between the ages of 40 to 60. The outcomes of data gathering and analysis were based on reviews from chosen respondents in interviews, surveys, and literature reviews. The target audience may easily comprehend the design visualization because it is a straightforward flat vector illustration. Therefore, it can be stated that this educational cartoon can be utilized to educate the public about the several types of cybercrime that exist in the modern period.*

Keywords: *APK files, cybercrime, cybersecurity awareness, online fraud cases.*

CC BY SA

PENDAHULUAN

Teknologi dan informasi semakin berkembang pesat dan mempermudah aspek-aspek kehidupan manusia saat ini. Keberadaan teknologi komunikasi yang ada, menjadikan manusia sebagai pribadi yang berpikir instan dan menemukan berbagai kemudahan tanpa memerlukan banyak waktu seperti dahulu (Marpaung, 2018). Internet dan teknologi juga berperan penting dalam menjawab kebutuhan-kebutuhan manusia dan memberikan dampak positif dalam kehidupan manusia, namun teknologi dan internet tersebut tidak hanya memberikan keuntungan saja melainkan juga dampak negatif, contohnya kejahatan siber (Budiastanti, 2017). Kejahatan siber atau dikenal juga sebagai *cybercrime* merupakan sebuah bentuk kejahatan berbasis komputer dengan tujuan kriminal seperti menghancurkan reputasi korban dan dapat menimbulkan kerugian dalam bentuk fisik maupun mental secara langsung atau tidak langsung (Andriani, 2023).

Sejak bulan Desember tahun 2022, laman web resmi Polri mencatat munculnya sebuah bentuk penipuan terbaru dengan cara mengirimkan sebuah file APK (*android package kit)* melalui fitur pesan pribadi kepada korban. Pelaku kejahatan mengirimkan file tersebut dengan pesan persuasif agar korban mengakses dan memasang sebuah aplikasi khusus yang dapat meretas, mencuri data-data pribadi, memata-matai, dan bahkan menguras saldo tabungan korban. Hal tersebut sangat mungkin terjadi karena saat mengakses *file* yang dikirimkan akan diminta izin atau data terkait akses ke berbagai aplikasi seperti email, SMS, foto, video, *m-banking*, dan lain-lain, sehingga aplikasi tersebut dapat memberikan berbagai kebutuhan data kepada pelaku kejahatan siber.

Kejahatan Siber (*Cybercrime*)

Kejahatan siber atau dikenal juga dengan *cybercrime* merupakan dampak negatif dari perkembangan teknologi dan informasi bagi kehidupan manusia (Agus, 2016). Kejahatan siber membentuk suatu opini di kalangan pengguna jasa internet karena merupakan sebuah tindakan yang merugikan orang lain dan melanggar hukum, serta dianggap sebagai sebuah tindakan amoral seperti yang ditulis oleh Ronda Hauben di dalam *The Declaration of the Rights of Netizen.* Kejahatan siber memiliki berbagai jenis antara lain: *cyberstalking*, *cyberterrorism, economic cybercrime*, dan lain-lain. Pengaruh dari kejahatan siber memiliki dampak yang besar dalam kehidupan manusia modern saat ini dan berhubungan erat dengan *"economic crime"*. Dengan demikian, kejahatan siber merupakan perbuatan menentang hukum atau peraturan yang didasari oleh teknologi dan jaringan telekomunikasi (Agus, 2016).

Cybersecurity Awareness

Kesadaran atau *awareness* memiliki arti memahami, mengetahui, dan menyadari situasi yang sedang terjadi di sekitar ataupun pada diri sendiri. Diperlukan suatu upaya untuk membangun kesadaran itu sendiri berupa ketertarikan, pemahaman,

dan merasakan hal-hal yang sedang terjadi di sekitar (Najahah dkk., 2022). Sedangkan *cybersecurity awareness* merupakan kemampuan dan pengetahuan seseorang dalam mempraktikkan keamanan ketika menggunakan jejaring internet, selain itu juga pengguna memahami pentingnya keamanan data pribadi dan memiliki upaya untuk melindungi data pribadi tersebut (Afandi dkk., 2017). Dengan kesadaran tersebut seseorang dapat terhindar atau mencegah hal-hal yang tidak diinginkan yang mungkin dapat terjadi. Namun, literasi dan informasi seputar keamanan data pribadi masih sedikit sehingga menimbulkan kebingungan dan ketidaktahuan tentang bagaimana cara menyikapi kejahatan siber (Hidayat dkk., 2023).

Kejahatan Siber Berbentuk File APK

Kementerian Komunikasi dan Informasi menerima banyak laporan mengenai kejahatan siber dari 2017 hingga 2022. Kominfo sendiri telah menerima sebanyak 486.000 laporan dari masyarakat dengan laporan transaksi elektronik yang mendominasi sebanyak 405.000 laporan (Kominfo, 2022). Kasus kejahatan siber menggunakan file APK saat ini sedang marak terjadi di dunia maya, pelaku kejahatan menggunakan modus berpura-pura sebagai orang-orang penting seperti aparat kepolisian dan menyebarkan surat tilang di aplikasi tertentu seperti Whatsapp, dengan mengganti judul pada pesan tersebut Surat Tilang yang berisikan sebuah file APK. Jika korban lengah atau kurang paham maka otomatis akan mengakses dan menginstal aplikasi yang sudah dimodifikasi oleh pelaku kejahatan siber sedemikian rupa sehingga data-data penting dan rahasia dari perangkat korban dapat dicuri (Kominfo, 2022).

Menurut Agus Prihanto, dosen Teknik Informatika Universitas Negeri Surabaya, penipuan seperti ini dilakukan dengan teknik *social engineering* atau rekayasa sosial yang memanfaatkan kelemahan dan psikologis korban, seperti kecerobohan, kepanikan, rasa penasaran, dan lain-lain. Pelaku kejahatan mengirimkan pesan yang bersifat persuasive dan semenarik mungkin agar korban melakukan apa yang dikehendaki oleh pelaku kejahatan siber. Pelaku kejahatan siber ini membuat aplikasi yang lebih banyak mengambil keuntungan daripada merusak sistem. APK ini juga menjadi sebuah aplikasi yang digunakan untuk memata-matai setiap aktivitas yang dilakukan oleh korban dan dapat mencatat informasi penting seperti *password, PIN,* dan lain-lain.

Modus kejahatan siber memiliki banyak jenis dengan tujuan dan target yang berbeda-beda. Berikut ini merupakan jenis-jenis kejahatan siber:

1. *Unauthorized Access to Computer System and Service*
   Kejahatan ini merupakan kegiatan menyelinap atau memasuki sistem komputer tanpa seizin atau sepengetahuan pemilik sistem yang dimasukinya. Umumnya *hacker* atau pelaku kejahatan memiliki tujuan atau maksud mencuri atau menyabotase data penting dan rahasia (Agus, 2016).
2. *Illegal Contents*
   Kejahatan ini merupakan kegiatan menyebarkan maupun memasukkan informasi maupun data ke dalam internet mengenai hal-hal yang non-etis,

tidak benar, dan dapat mengganggu ketertiban umum maupun melanggar hukum yang ada. Contohnya adalah sebuah berita bohong atau lebih dikenal sebagai hoaks yang memiliki tujuan mencoreng nama baik atau menjatuhkan martabat dan harga diri pihak tertentu, hal-hal seputar pornografi, propaganda yang bertujuan untuk melawan pemerintahan atau aturan yang sah, dan lain-lain (Agus, 2016).

3. *Data Forgery*
   Kejahatan ini adalah sebuah bentuk kejahatan memalsukan dokumen atau data-data penting. Kejahatan ini umumnya ditargetkan pada dokumen-dokumen atau data *e-comers* dengan skenario seperti terjadi "salah ketik" dan pada akhirnya akan memberikan keuntungan bagi pelaku (Agus, 2016).
4. *Cyber Espionage*
   Kejahatan ini merupakan bentuk kejahatan yang memanfaatkan internet dengan tujuan melakukan sebuah kegiatan mata-mata kepada pihak lain, menggunakan cara memasuki sebuah sistem jaringan komputer pihak sasaran. Kejahatan ini umumnya ditujukan kepada saingan bisnis yang dokumen atau data pentingnya disimpan dalam suatu sistem *database* (Agus, 2016).
5. *Cyber Sabotage and Extortion*
   Kejahatan ini merupakan bentuk kejahatan yang merusak, mengganggu, atau perusakan akan suatu data komputer maupun sistem komputer yang tersambung dengan internet. Umumnya kejahatan ini memasukkan sebuah virus atau program tertentu sehingga jaringan sistem komputer atau program komputer tidak berjalan dengan benar sebagaimana mestinya. Lalu pelaku kejahatan dengan sengaja menawarkan diri kepada korban dengan tujuan memperbaiki sistem komputer tersebut tentunya dengan bayaran yang cukup tinggi (Agus, 2016).
6. *Offense Against Intellectual Property*
   Kejahatan ini merupakan bentuk kejahatan yang menargetkan kekayaan atau hak yang dimiliki pihak lain di dalam internet. Contohnya plagiarisme tampilan media sosial atau web yang dimiliki pihak lain tanpa seizin atau sepengetahuan pihak tersebut secara ilegal, atau penyebaran informasi yang merupakan rahasia dagang pihak lain (Agus, 2016).
7. *Infringements of Privacy*
   Kejahatan ini merupakan bentuk kejahatan yang menargetkan data atau informasi orang lain yang bersifat privasi atau bersifat pribadi maupun rahasia. Umumnya kejahatan ini menargetkan data pribadi yang terdapat di dalam formulir data pribadi dan disimpan secara *computerized* apabila diketahui oleh orang lain dapat merugikan korban secara material maupun imaterial, contohnya PIN ATM, nomor kartu kredit, dan lain-lain (Agus, 2016).
8. *Carding*
   Kejahatan ini merupakan bentuk kejahatan yang memanfaatkan teknologi komputer untuk melakukan transaksi menggunakan kartu ATM atau kredit tanpa seizin dan sepengetahuan korban sehingga dapat merugikan korban secara material maupun immaterial (Agus, 2016).

Rekayasa Sosial (*Social Engineering)*

Terdapat sebuah prinsip yang berbunyi "*the strength of a chain depends on the weakest link*" atau diartikan sebagai kekuatan sebuah rantai bergantung pada sambungan terlemahnya. Dalam hal ini sambungan terlemah yang dimaksud merupakan manusia itu sendiri karena meskipun sebuah perangkat sudah memiliki beragam teknologi canggih seperti *firewall, antivirus,* dan lain-lain namun faktor pengendali utamanya yakni manusia tetap memegang peranan penting. Konsep inilah yang dimanfaatkan oleh pelaku kejahatan dalam aksinya untuk mendapatkan keuntungan. Oleh karena itu, pelaku kejahatan menggunakan teknik yang dikenal sebagai rekayasa sosial atau "*social engineering*" (Indrajit, 2017). *Social engineering* sendiri adalah teknik yang sering digunakan oleh pelaku kejahatan siber untuk memperoleh informasi penting yang bersifat rahasia dengan melakukan pendekatan yang manusiawi seperti mengeksploitasi psikologis manusia dan memanfaatkan kelemahannya seperti memanfaatkan rasa takut, penasaran, ingin menolong, percaya, dan lain-lain (Junaedi, 2017).

Digital Immigrants

Sekarang ini kelompok masyarakat terbagi menjadi dua yaitu generasi *digital natives* dan *digital immigrants.* Generasi *digital immigrants* merupakan kelompok masyarakat yang terlahir sebelum tahun 1980 yang tidak terbiasa dengan teknologi karena terlahir ketika internet dan teknologi belum berkembang dengan pesat, sedangkan generasi *digital natives* merupakan kelompok masyarakat yang terlahir setelah tahun 1980 saat teknologi dan informasi sedang berkembang dengan pesat. Generasi *digital natives* ini terbiasa dengan teknologi dan memiliki kecakapan menggunakan teknologi berbasis digital. Di Indonesia sendiri teknologi dan informasi baru berkembang dengan pesat pada tahun 1994 berbeda dengan negara maju yang sudah lebih dahulu memiliki perkembangan internet dan teknologi (Nurhadrayani dkk., 2017). Generasi *digital immigrants* secara natural memiliki kesulitan dalam mempelajari teknologi dan menganggap teknologi merupakan penemuan terbaru yang sulit diterima (Apidana dkk., 2020). Oleh karena itu, target penelitian ini dibatasi dengan masyarakat Indonesia yang terlahir sampai dengan sebelum tahun 1994 karena generasi ini tidak terbiasa menggunakan teknologi dan merupakan generasi yang memiliki risiko tinggi terkena penipuan.

Berdasarkan pemaparan beberapa referensi di atas, dapat diketahui bahwa belum ada penelitian sejenis yang mengangkat isu kejahatan siber yang difokuskan pada masyarakat Indonesia berusia 40-60 tahun. Hal ini menjadikan penelitian ini memiliki kebaruan dibandingkan penelitian sejenis lainnya karena hasil akhir melibatkan sebuah perancangan animasi sebagai media informasi sekaligus edukasi terkait variasi kejahatan siber dan upaya menanggulanginya.

METODE

Jenis penelitian yang dilakukan menggunakan metode pendekatan *mix-method* dengan pendekatan *glass box* (Usman, 2021) (Afriwan, 2018) (Evan, Natanael, Aryani, 2022) untuk menyelidiki dan mengetahui makna dari masalah sosial atau kemanusiaan (Creswell, 2016) (Wahyudi, Kalbuadi, Pertiwi, 2022) yang saat ini sedang terjadi yakni terkait kejahatan siber. Penelitian *mix-method* dilakukan dengan pendekatan pengumpulan data secara kuantitatif melalui kuesioner/ survey serta hasil olah data wawancara dengan sampling responden serta studi literatur untuk menentukan strategi empiris komparatif konsep perancangan berdasarkan konsep animasi sederhana. Tujuan akhir dari penelitian ini adalah mengedukasi masyarakat Indonesia dalam menyikapi maraknya kasus penipuan *online* berbasis file APK sesuai dengan pengalaman maupun kondisi nyata dalam masyarakat Indonesia dewasa ini. Pengumpulan data awal dilakukan melalui kajian literatur sejalan dengan penelitian sejenis yakni tentang kejahatan siber, selanjutnya data informasi dari hasil mengolah kuesioner kepada target responden berusia 40-60 tahun, serta studi literature berupa data tambahan pelengkap data primer yang berhubungan dengan topik yang dikaji. Adapun dalam pengumpulan data kuantitatif melalui kuesioner/survey dibatasi pada 100 orang responden berusia minimal 30 tahun di wilayah Bandung dan Jabodetabek (Jakarta-Bogor-Depok-Tangerang-Bekasi) dengan pertimbangan kedua wilayah tersebut memiliki gaya hidup khas kota besar yang hampir sama serta memiliki akses dan aktif dalam media sosial pada gawai, teknik yang dipilih dalam pengumpulan sampel adalah *purposive sampling* untuk mencari sampel yang sesuai dengan kriteria ruang lingkup penelitian dan memiliki nilai representatif untuk mengetahui jawaban serta pendapat responden mengenai kejahatan *online* berbentuk file APK.

Hasil Kuesioner

Berdasarkan beberapa pertanyaan yang diajukan kepada responden, dengan memiliki sistem skala poin 1-5 dengan catatan poin 1 merupakan poin terendah dan poin 5 merupakan poin tertinggi ditampilkan dalam beberapa tabel sebagai berikut:

Tabel 1. Pengetahuan responden tentang kejahatan siber
Sumber: dokumentasi Nikkolas Fassa (2023)

Poin	Jumlah Responden
1- Sangat Tidak Tahu	7 orang (7%)
2- Tidak Tahu	14 orang (14%)
3- Ragu-ragu	39 orang (39%)
4- Tahu	25 orang (25%)
5- Sangat Tahu	15 orang (15%)

Merujuk pada tabel 1, dapat diketahui bahwa mayoritas responden menjawab poin 3 yaitu ragu-ragu sebanyak 39 orang dan dapat disimpulkan bahwa pengetahuan responden seputar kejahatan siber belum terlalu banyak ataupun sudah mengetahui namun tidak memiliki dasar literasi atau informasi yang pasti.

Tabel 2. Pendapat responden tentang kejahatan siber
Sumber: dokumentasi Nikkolas Fassa (2023)

Pertanyaan tentang kejahatan siber	Keterangan	Jumlah Responden
Kejahatan siber adalah tindakan kriminal yang dilakukan menggunakan teknologi	Benar	79 orang (79%)
Kejahatan siber merupakan kejahatan menggunakan handphone	Salah	34 orang (34%)
Seseorang bisa terkena kejahatan siber jika membalas atau memberi respon	Benar	34 orang (34%)
Ancaman siber berasal dari pihak luar (*hacker*, virus, dan lain-lain)	Salah	24 orang (24%)
Password yang rumit akan menjaga keamanan data dan peralatan	Salah	80 orang (80%)

Pada pertanyaan yang ditampilkan Tabel 2, responden dapat memilih lebih dari satu pernyataan untuk mengetahui sejauh mana pemahaman responden mengenai kejahatan siber dan diperoleh hasil seperti di atas. Dengan demikian dapat disimpulkan bahwa pengetahuan responden seputar kejahatan siber masih minim.

Tabel 3. Pengalaman responden terkait kejahatan siber
Sumber: dokumentasi Nikkolas Fassa (2023)

Pernah atau Tidak Pernah	Jumlah Responden
Pernah	36 orang (36%)
Tidak Pernah	64 orang (64%)

Merujuk pada tabel 3, pertanyaan yang diajukan berupa pengalaman responden tentang pernah atau tidaknya terkena kejahatan siber, yang ditunjukkan sebanyak 64% responden tidak pernah terkena kejahatan siber. Hal ini menunjukkan mayoritas responden memiliki risiko tinggi terkena kejahatan siber karena tidak memiliki pengalaman.

Tabel 4. Pendapat responden tentang file APK secara umum
Sumber: dokumentasi Nikkolas Fassa (2023)

Pernyataan tentang file APK	**Keterangan**	**Jumlah Responden**
File APK merupakan file untuk menginstall aplikasi	Benar	43 orang (43%)
File APK merupakan file gambar	Salah	9 orang (9%)
File APK merupakan sebuah aplikasi	Benar	25 orang (25%)
Tidak Tahu	Salah	34 orang (34%)

Merujuk pada tabel 4 di atas, mayoritas responden menjawab pernyataan yang benar sebanyak 43% namun angka responden yang menjawab tidak tahu cukup banyak yaitu 34%.

Tabel 5. Kesadaran responden tentang penipuan berbentuk file APK
Sumber: dokumentasi Nikkolas Fassa (2023)

Kesadaran Responden terhadap Penipuan Berbentuk File APK	**Jumlah Responden**
Tahu	52 orang (52%)
Tidak Tahu	48 orang (48%)

Merujuk pada tabel 5, mayoritas responden menjawab sudah mengetahui tentang kejahatan siber berbentuk file APK.

Tabel 6. Kesadaran responden tentang jenis kejahatan siber
Sumber: dokumentasi Nikkolas Fassa (2023)

Jenis Kejahatan Siber	**Jumlah Responden**
Phising	45 orang (45%)
Cracking	27 orang (27%)
Cyber Bullying	53 orang (53%)
Cyber Stalking	37 orang (37%)
Lain-lain	6 orang (6%)

Merujuk pada tabel 6, kejahatan siber yang paling banyak diketahui oleh responden yaitu *cyberbullying* sebanyak 53%.

Tabel 7. Cara responden mengantisipasi kejahatan siber
Sumber: dokumentasi Nikkolas Fassa (2023)

Cara Mengantisipasi Kejahatan siber	Jumlah Responden
Membuat *password* yang rumit	63 orang (63%)
Menggunakan *antivirus*	33 orang (33%)
Membuat cadangan data	29 orang (29%)
Melakukan *update*	37 orang (37%)
Lain-lain	12 orang (12%)

Merujuk pada tabel 7, menunjukkan cara mengantisipasi kejahatan siber yang paling banyak dipilih oleh responden adalah membuat *password* yang sulit sebanyak 63%. Namun, *password* yang sulit saja tidak cukup untuk menjaga keamanan karena kejahatan siber bisa menyerang dari berbagai faktor seperti faktor psikologis manusia, kecanggihan perangkat teknologi, dan lain-lain.

Tabel 8. Pendapat responden tentang porsi informasi kejahatan siber di Indonesia
Sumber: dokumentasi Nikkolas Fassa (2023)

Poin	Jumlah Responden
1- Sangat Tidak Cukup	48 orang (48%)
2- Tidak Cukup	23 orang (23%)
3- Ragu-ragu	21 orang (21%)
4- Cukup	4 orang (4%)
5- Sangat Cukup	4 orang (4%)

Merujuk pada tabel 8, mayoritas responden menjawab poin 1 yaitu sangat tidak cukup tentang informasi kejahatan siber di Indonesia. Hal ini menunjukkan bahwa memang masyarakat sudah sadar terkait minimnya informasi dan edukasi seputar kejahatan siber.

Tabel 9. Pendapat responden tentang informasi dan edukasi seputar kejahatan siber
Sumber: dokumentasi Nikkolas Fassa (2023)

Poin	Jumlah Responden
1- Sangat Tidak Penting	-
2- Tidak Penting	-
3- Ragu-ragu	21 orang (21%)
4- Penting	27 orang (27%)
5- Sangat Penting	52 orang (52%)

Merujuk pada tabel 9, mayoritas responden menjawab poin 5 yaitu sangat penting. Dengan demikian dapat disimpulkan bahwa diperlukan suatu media informasi dan edukasi yang sesuai dengan kondisi demografis dan psikologis masyarakat Indonesia terkait kejahatan siber.

HASIL DAN PEMBAHASAN

Berdasarkan hasil kuesioner dan observasi dari responden terpilih didapatkan hasil bahwa sebagian besar pernah mendapatkan kiriman pesan berisi aplikasi file APK yang mengatasnamakan pihak tertentu. Hal tersebut mempengaruhi rasa penasaran, takut, panik, serta berpengaruh terhadap kondisi psikologis dan kualitas hidup mereka. Berdasarkan pemaparan tabel-tabel dari hasil olah data kuesioner diperoleh hasil bahwa masih banyak responden yang belum mengetahui tentang berbagai bentuk kejahatan siber, khususnya tindakan penipuan berbasis file APK. Hasil kuesioner juga menunjukkan bahwa responden mengharapkan adanya sebuah media yang dapat memfasilitasi informasi dan edukasi tentang bentuk-bentuk kejahatan siber serta cara penanggulangannya.

Konsep Komunikasi

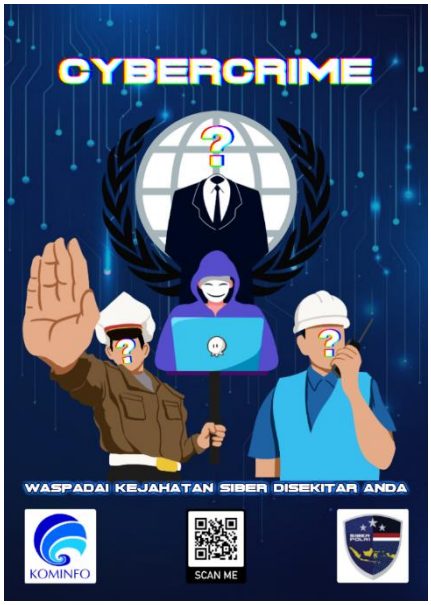
Seiring berkembangnya teknologi dan informasi, kasus penipuan *online* semakin marak terjadi akibat kemudahan bagi pelaku kejahatan siber untuk melakukan aksinya. Saat ini, muncul kasus penipuan *online* terbaru yang menimbulkan kehebohan dunia maya yaitu kasus penipuan *online* menggunakan file APK. Kasus penipuan ini tercatat muncul pada bulan Desember 2022 dan telah memakan banyak korban karena minimnya informasi atau edukasi seputar keamanan data atau kejahatan siber melalui cara-cara yang tidak terduga. Berdasarkan permasalahan tersebut, diperlukan sebuah media informasi dan edukasi bagi masyarakat terhadap bahayanya kejahatan siber agar masyarakat terhindar dari kejahatan siber. Gaya komunikasi yang digunakan dalam perancangan animasi ini menggunakan bahasa sehari-hari yang bersifat semiformal dengan pertimbangan target karya ditujukan kepada generasi *digital immigrants* yang berusia antara 40-60 tahun.

Konsep Kreatif

Target utama dari perancangan ini adalah masyarakat dewasa di Indonesia yang berusia 40-60 tahun dengan memiliki akses terhadap media sosial dan internet. Oleh karena itu, perancangan yang dilakukan berupa media edukatif berbentuk video animasi dengan pendekatan visual ilustrasi digital disebut *flat design vector*. Pemilihan *flat design vector* sebagai konsep kreatif utama karena gaya ini memiliki impresi atau kesan akrab agar target penonton merasa tertarik dan tidak bosan sehingga hal-hal yang disampaikan dapat berkesan realistis, edukatif, dan informatif. Selanjutnya, video animasi menggunakan gaya animasi *motion graphic* yaitu jenis animasi yang dikenal tanpa cerita dan juga terkenal efektif dalam menyampaikan informasi karena mudah dipahami dan sederhana.

Konsep Media

Media merupakan suatu alat untuk menyampaikan informasi atau pesan kepada penerima, sering kali digunakan dalam proses belajar mengajar karena media memiliki tingkat efektivitas tinggi dalam pelaksanaannya. Media yang digunakan untuk tujuan pembelajaran juga dikenal sebagai media pembelajaran, perkembangan teknologi dan ilmu pengetahuan memiliki pengaruh besar pada media pembelajaran yang dapat memberikan informasi bagi penerima dengan baik, efisien, dan efektif (Muhson, 2010). Dengan demikian, media utama yang dipilih untuk menyebarkan video animasi edukatif ini adalah Youtube karena merupakan sebuah *platform* yang fleksibel dan mudah diakses oleh banyak orang. Youtube merupakan media yang tepat untuk penyebaran video animasi secara masif, selanjutnya dibuat pula media promosi tambahan berupa poster dan *flyer* yang berisi *QR code* untuk mengarahkan target langsung membuka video melalui *scanning*. Media tambahan yang dirancang ditujukan sebagai bagian dari sosialisasi kepada masyarakat, dengan melampirkan informasi dari mandatory terkait yakni Cyber Polri dan Kominfo.



Gambar 1. Poster untuk sosialisasi kejahatan siber kepada masyarakat
Sumber: dokumentasi Nikkolas Fassa (2023)

Media poster yang dibuat berukuran A2 dengan visualisasi tiga figur yakni di bagian tengah seorang *hacker* yang dapat mengatasnamakan dirinya menjadi berbagai pihak penting seperti polisi (kiri) dan petugas PLN atau telekomunikasi (kanan) untuk mengelabui masyarakat. Figur yang digambarkan memiliki gambaran tubuh manusia dengan bagian kepalanya divisualisasikan secara *flat* dan terdapat simbol tanda tanya untuk memberikan kesan misterius dan tidak dapat dipercaya sebagaimana penggambaran karakter tokoh jahat atau tidak baik (Aryani, 2021). Pada poster terdapat *tagline* "Waspadai kejahatan siber di sekitar Anda" dengan tujuan bahwa beberapa skenario kejahatan yang terjadi saat ini akibat target atau calon korban terkadang terlalu mempercayai pesan dari orang yang tidak

dikenal. Oleh karena itu, *tagline* ini menjadi pengingat bagi masyarakat untuk perlu meningkatkan kewaspadaan.

Gambar 2. Flyer untuk sosialisasi kejahatan siber kepada masyarakat
Sumber: dokumentasi Nikkolas Fassa (2023)

Adapun media tambahan lainnya berupa *flyer* berukuran A5 dan memiliki visualisasi seorang *hacker* dengan *background* gelap yang bertujuan memberikan kesan misterius. Media promosi *flyer* ini akan diberikan secara cuma-cuma kepada masyarakat yang mengikuti kegiatan sosialisasi supaya mengingatkan masyarakat agar selalu berhati-hati terhadap kejahatan siber di sekitarnya.

Media utama perancangan ini berupa video animasi diawali dengan logo sebagai berikut:

Gambar 3. Logo video animasi Cybercrime
Sumber: dokumentasi Nikkolas Fassa (2023)

Terdapat dua *font* utama dalam pembuatan logo animasi yaitu Fough Knight X sebagai Logo karena memiliki kesan futuristik yang cocok dengan topik permasalahan. *Font* Montserrat Bold sebagai *subtitle* dipilih karena memiliki tingkat keterbacaan yang jelas sehingga cocok dijadikan sebagai *subtitle* sepanjang animasi ditayangkan.

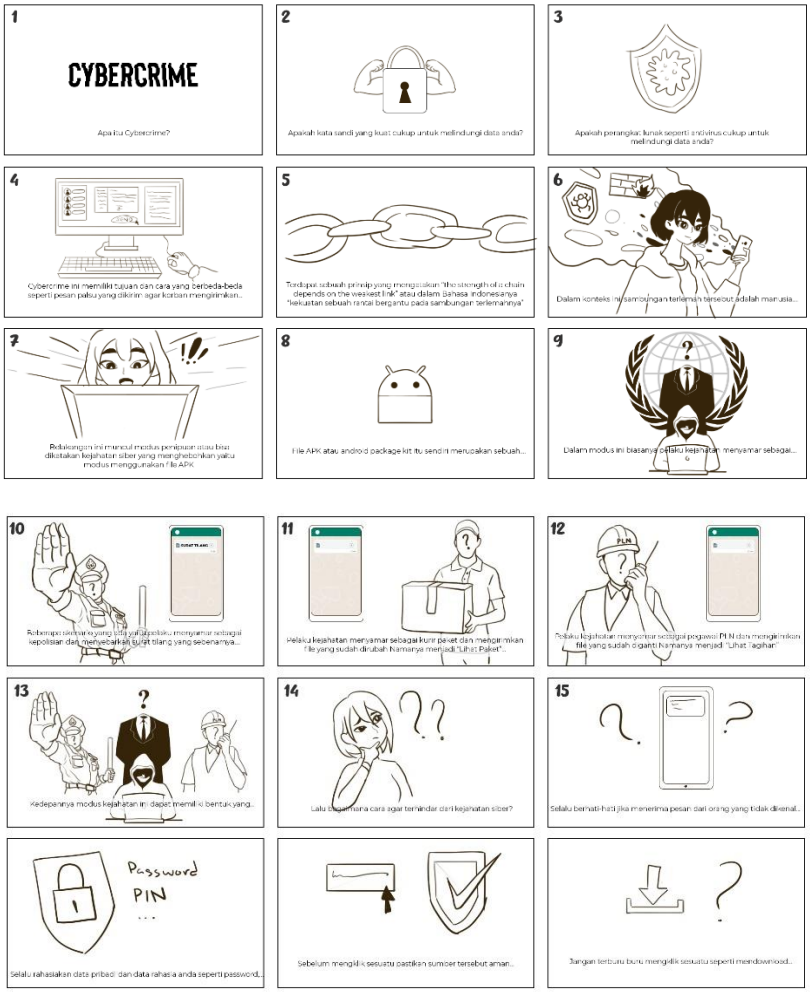
Gambar 4. *Font* Fough Knight X
Sumber: dokumentasi Nikkolas Fassa (2023)

Gambar 5. *Font* Montserrat Bold
Sumber: dokumentasi Nikkolas Fassa (2023)

Adapun warna yang digunakan dalam perancangan video animasi berupa warna-warna *colourful* dan *vibrant* dengan tujuan menarik minat penonton sehingga penonton mau mengikuti video animasi yang ditayangkan hingga selesai. Selain itu, penggunaan warna-warna tersebut mampu menarik fokus penonton agar informasi dapat tersampaikan dengan baik.

Gambar 5. Palet warna dan contoh penggunaannya dalam salah satu *scene* animasi
Sumber: dokumentasi Nikkolas Fassa (2023)

Perancangan video animasi tentang kejahatan siber diawali dengan pembuatan konsep awal melalui *storyboard* sebanyak dua halaman sebagai berikut:



Gambar 6. Konsep *storyboard* video animasi
Sumber: dokumentasi Nikkolas Fassa (2023)

Berdasarkan dua halaman *storyboard* di atas selanjutnya dibuat menjadi empat seri video animasi. Seri pertama memberikan informasi dan pengertian seputar kejahatan siber secara umum, terdapat beberapa pertanyaan pada awal video yang mungkin belum diketahui oleh penonton untuk memicu rasa penasaran atau keingintahuan. Seri kedua menunjukkan informasi seputar file APK itu sendiri yang bertujuan agar penonton paham bagaimana cara pelaku kejahatan melakukan aksinya. Seri ketiga menunjukkan skenario penipuan menggunakan file APK yang dilakukan oleh pelaku kejahatan siber, serta seri keempat menunjukkan informasi edukatif tentang cara penanggulangan agar terhindar dari kejahatan siber.

Video Seri Pertama

Video animasi seri pertama berisi tentang informasi dasar seputar kejahatan siber yang dibuat dengan tujuan agar penonton memahami apa itu kejahatan siber.

Gambar 7. Cuplikan video animasi seri pertama – Apa itu *Cybercrime*?
Sumber: dokumentasi Nikkolas Fassa (2023)

Video Seri Kedua

Video animasi seri kedua berisi tentang informasi dasar seputar file APK dan cara pelaku kejahatan menggunakan file APK untuk menjebak calon target atau korbannya.

Gambar 8. Cuplikan video animasi seri kedua – Modus Penipuan Menggunakan File APK
Sumber: dokumentasi Nikkolas Fassa (2023)

Video Seri Ketiga

Video animasi seri ketiga berisi tentang informasi modus-modus penipuan menggunakan file APK yang sekarang ini sedang marak terjadi. Seri ketiga ini bertujuan agar penonton mengetahui cara yang digunakan oleh pelaku kejahatan dalam melakukan aksinya.

Gambar 9. Cuplikan video animasi seri ketiga – Skenario Modus Penipuan Berbasis File APK
Sumber: dokumentasi Nikkolas Fassa (2023)

Video Seri Keempat

Video animasi seri keempat berisi informasi seputar cara pencegahan agar tidak terkena kejahatan siber. Pada seri ini menampilkan informasi dasar agar terhindar dari kejahatan siber yang diharapkan dapat menjadi acuan dasar bagi masyarakat, serta dapat mengubah pola pikir dan tindakan yang perlu dilakukan jika berada dalam kondisi tersebut.

Gambar 10. Cuplikan video animasi seri keempat – Cara penanggulangan kejahatan siber
Sumber: dokumentasi Nikkolas Fassa (2023)

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan terkait kejahatan siber berbasis *file* APK dewasa ini, dapat disimpulkan bahwa masih kurangnya pemahaman masyarakat mengenai kejahatan siber. Seiring dengan berkembangnya teknologi dan informasi yang memudahkan bagi pelaku kejahatan untuk menjebak korban-korbannya, juga minimnya informasi seputar kejahatan siber di Indonesia menjadi

salah satu faktor penyebab maraknya kasus penipuan online berbasis *file* APK dewasa ini. Oleh karena itu, untuk meningkatkan pengetahuan dan *awareness* masyarakat terhadap isu tersebut, diperlukan suatu media yang tepat dan mudah atau dapat diakses oleh siapapun serta di manapun melalui gawai. Video animasi dengan jenis *motion graphic* sering digunakan sebagai media pembelajaran edukatif. Konsep itulah yang digunakan sebagai landasan perancangan video animasi yang berisi informasi seputar kejahatan siber dengan gaya *flat design vector* berwarna *colorful* dan *vibrant* yang terbagi ke dalam empat seri video pendek terbukti efektif dalam kemudahannya menyampaikan informasi dan mengedukasi masyarakat, dalam hal ini generasi *digital immigrant* yang berusia 40-60 tahun untuk lebih mudah mengerti dan memahami isi video.

DAFTAR PUSTAKA

Afandi, I. A., Kusyanti, A., & Wardani, N. H. (2017). Analisis Hubungan Kesadaran Keamanan, Privasi Informasi, dan Perilaku Keamanan Pada Para Pengguna Media Sosial Line. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, 1(9), 783–792.

Afriwan, H. dan Mila. (2018). *Redesign Sign System Penangkaran Penyu di Pariaman* (laporan tugas akhir). Padang: Prodi DKV UNP.

Agus, A. A., & Riskawati, R. (2016). Penanganan Kasus Cyber Crime Di Kota Makassar (Studi Pada Kantor Kepolisian Resort Kota Besar Makassar). *SUPREMASI: Jurnal Pemikiran, Penelitian Ilmu-ilmu Sosial, Hukum dan Pengajarannya*, 11(1).

Andriani, N. (2023). Cybercrime Kejahatan Yang Berbasis Komputer. *Jurnal Hukum Non Diskriminatif (JHND)*, 1(2), 55-63.

Apidana, Y. H., Suroso, A., & Setyanto, R. P. (2020). Model Penerimaan Teknologi Mobile Payment Pada Digital Native Dan Digital Immigrant Di Indonesia. *Jurnal Ekonomi, Bisnis, dan Akuntansi*, 21(4), 1-16. DOI: https://doi.org/10.32424/jeba.v21i4.1542.

Aryani, D. I. (2021). *Menguak Karakter dan Visualisasi Eevee dalam Franchise Pokemon*. Banyumas: Amerta Media.

Budiastanti, D. E. (2017). Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Melalui Internet. *Jurnal Cakrawala Hukum*, 8(1), 22-32.

Creswell, J. W. (2016). *Research Design Pendekatan Metode Kualitatif, Kuantitatif, dan Campuran*. Yogyakarta: Pustaka Pelajar.

Evan, D.M., Natanael, I.N., Aryani, D.I. (2022). Perancangan Konten Digital Edukasi Tentang Anti "Food Waste" Melalui Video Animasi. *dekave: Jurnal Desain Komunikasi Visual* 12(3), 235-246. DOI: https://doi.org/10.24036/dekave.v12i3.117939.

Hidayat, F. P., Hardiyanto, S., Lubis, F. H., Adhani, A., & Zulfahmi, Z. (2023). Kemampuan Literasi Media Sebagai Upaya Mengantisipasi Cybercrime Pada Remaja Di Kota Medan. *Jurnal Interaksi: Jurnal Ilmu Komunikasi*, 7(1), 13-25.

Indrajit, R. E., & Teknik, S. B. (2017). Social Engineering. *SERI*, *999*, *6*.

Junaedi, D. I. (2017). Antisipasi Dampak Social Engineering Pada Bisnis Perbankan. *Infoman's*, 11(1), 1-10.

Kominfo Indonesia. (2022). Laporan Tahunan Kementrian Komunikasi dan Informatika Tahun 2021. *KOMINFO*. Retrieved February 20, 2023, from https://web.kominfo.go.id/sites/default/files/users/70/Laptah2021.pdf.

Marpaung, J. (2018). Pengaruh penggunaan gadget dalam kehidupan. *KOPASTA: Journal of the Counseling Guidance Study Program*, 5(2). DOI: https://doi.org/10.33373/kop.v5i2.1521.

Muhson, A. (2010). Pengembangan Media Pembelajaran Berbasis Teknologi Informasi. *Jurnal Pendidikan Akuntansi Indonesia*, 8(2), 1-10. DOI: https://doi.org/10.21831/jpai.v8i2.949.

Najahah, N., Nurkholida, E., & Ulfah, U. N. M. R. (2022). Examining Student's Awareness And Behavior In Dealing With Virtual Learning Environment. *Fenomena*, 21(1), 1-18.

Nurhadryani, Y., Hutomo, Y. S., Kurnia, A., Anisa, R., & Ramadhan, D. A. (2017). Karakteristik Digital Native dan Digital Immigrant Masyarakat Bogor Menuju E-government. *Seminar Nasional Sistem Informasi Indonesia (SESINDO) 9*, November 2017.

Usman, M. (2021). MOTION GRAPHIC WASPADA PENYEBARAN HOAX DI SOSIAL MEDIA. *DEKAVE*, 11(3), 303-311. DOI: https://doi.org/10.24036/dekave.v11i3.114590.

Wahyudi, L., Kalbuadi, G., & Pertiwi, E. (2022). PERANCANGAN ANIMASI 3D IKLAN LAYANAN MASYARAKAT KAMPANYE SOSIAL VAKSINASI COVID-19 DI BANYUMAS. *Demandia: Jurnal Desain Komunikasi Visual, Manajemen Desain, Dan Periklanan*, 7(2), 181-202. doi:10.25124/demandia.v7i2.4595.