

DigiTimes #32
JUNI 2020

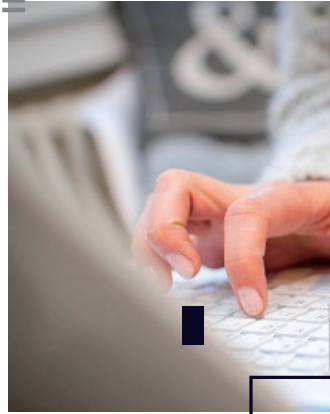
PENINGKATAN KOMPETENSI KEAMANAN DIGITAL DI INDONESIA:

ANALISIS REKAYASA PENIPUAN
DENGAN TEKNIK REKAYASA SOSIAL



CfDS
CENTER FOR DIGITAL SOCIETY

Room BC 201- 202
Faculty of Social and Political Sciences
Universitas Gadjah Mada
Jalan Sosio Yustisia 1, Bulaksumur, Yogyakarta
(0274) 563362, Ext. 116 | cfds.fisipol@ugm.ac.id



PENULIS
DAN KONTRIBUTOR

Penulis

Anaq Duanaiko
Janitra Haryanto
Paska Bayu Darmawan
Yuliana Khong

Editor

Anisa Pratita Kirana Mantovani

Desain dan Tata Letak

Naufal A. Radityasakti

JUNI 2020

■ DAFTAR ISI

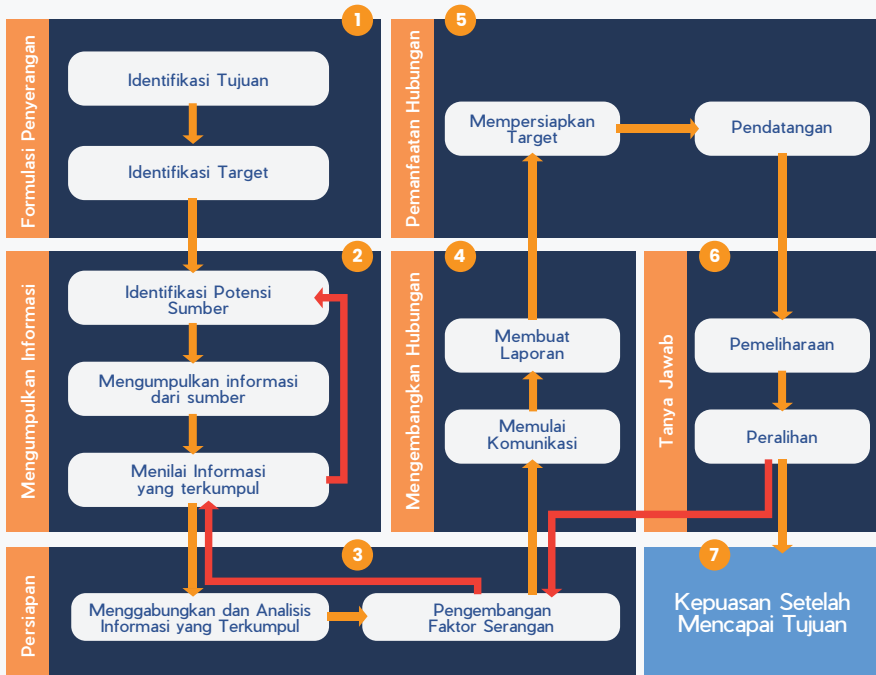
2	Pengantar
4	Perkembangan Kasus Penipuan dengan Teknik Rekayasa Sosial di Indonesia
9	Kompetensi Keamanan Teknologi Digital Tingkat Dasar (<i>Basic</i>)
9	Kompetensi Keamanan Teknologi Digital Tingkat Menengah (<i>Intermediate</i>)
10	Kompetensi Keamanan Teknologi Digital Tingkat Lanjutan (<i>Advanced</i>)
11	Rekomendasi Pencegahan Penipuan dengan Teknik Rekayasa Sosial: Pendidikan, Pelatihan, dan Peningkatan Kesadaran
12	• Industri Teknologi
14	• Pemerintah dan Regulator
15	• Organisasi Masyarakat
16	• Akademisi
18	• Individu
20	Kesimpulan
21	Referensi



■ PENGANTAR

Dewasa ini, semakin pesatnya perkembangan teknologi yang dibarengi oleh kegiatan ekonomi di ranah digital berimbas pada meningkatnya angka kriminalitas. Salah satunya adalah penipuan dengan teknik rekayasa sosial. Penipuan ini menggunakan kemampuan pelaku untuk membangun kepercayaan korban dan memanfaatkan kepercayaan tersebut untuk melaksanakan serangan tipuannya.¹

Teknik rekayasa sosial seringkali tidak memanfaatkan kelemahan suatu sistem elektronik, melainkan memanfaatkan kelemahan pengguna sebagai pihak yang memiliki otoritas dalam sistem elektronik tersebut. Penipuan dengan teknik rekayasa sosial yang dimaksud dalam kajian ini merujuk pada penipuan dengan teknik rekayasa sosial dengan motif ekonomi yang dilakukan di berbagai macam sektor.



Grafik 1. Kerangka penyerangan penipuan dengan rekayasa sosial.²

Melihat dari kerangka penyerangan penipuan di atas, formulasi penyerangan merupakan langkah pertama dengan melakukan identifikasi tujuan penipuan dan target. Kedua, tahap mengumpulkan informasi dengan identifikasi potensi sumber, mengumpulkan informasi dari sumber, lalu menilai informasi yang terkumpul. Jika sekiranya masih kurang, pelaku akan kembali mengidentifikasi hingga sesuai dengan apa yang telah diformulasikan di awal.

Ketiga, pelaku penyerangan akan mengumpulkan persiapan dengan menggabungkan dan analisis informasi yang telah terkumpul, lalu

mengembangkan faktor serangan. Keempat, pelaku akan mulai mengembangkan hubungan dengan korban dengan memulai komunikasi dan membangun kepercayaan. Kelima, pelaku akan mulai memanfaatkan hubungan dengan mempersiapkan target yang akan secara paksa diambil informasinya. Keenam, proses tanya jawab akan dilakukan untuk memelihara hubungan hingga pada peralihan untuk eksekusi, jika sekiranya masih kurang, pelaku akan melakukan persiapan agar lebih matang. Apabila eksekusi sudah dianggap cukup, pelaku akan mencapai tujuan yang telah diformulasikan di awal.



■ PERKEMBANGAN KASUS PENIPUAN DENGAN TEKNIK REKAYASA SOSIAL DI INDONESIA

Dalam kajian ini, penulis mengambil data berupa berita online yang dilakukan dari tahun 2013 hingga akhir 2019. Penulis menggunakan beberapa kata kunci yang berkaitan dengan penipuan dengan teknik rekayasa sosial seperti: *penipu*, *scam*, *fraud*, *bodong* dan sebagainya. Sedangkan kata kunci yang berkaitan dengan *fintech* meliputi *e-wallet*. Berdasarkan hasil pengambilan data tersebut kajian ini mengelompokkan kasus dan modus penipuan menjadi dua bagian yaitu modus rekayasa sosial sebelum *fintech* menjadi populer, yakni dari tahun 2013 hingga 2017 dan setelah *fintech* menjadi populer pada tahun 2018 hingga 2019.

Selama tahun 2013-2017, kasus-kasus penipuan rekayasa sosial tidak menargetkan pengguna *fintech* sampai tahun 2018. Modus-modus yang ditemukan adalah undian berhadiah berkedok polisi, pejabat, pihak bank dan provider selular, juga *Advance-fee scam* (sindikatis *Nigerian scam* melalui broadcast melalui aplikasi olah pesan) serta peretasan email perusahaan. Sedangkan selama tahun 2014 terdapat modus lainnya yaitu pemalsuan *website* dan *phishing*. Selama tahun 2015 beberapa kasus penipuan seperti undian berhadiah, *phishing malware* masih terjadi ditambah dengan kasus penipuan investasi emas dan “mama minta pulsa”.



Untuk tahun 2016, kasus *advance-fee scam* kembali terjadi menasar perempuan di sebuah media jejaring sosial ditambah dengan kasus pembobolan internet banking dengan modus kartu sim rusak. Sedangkan pada tahun 2017, kasus rekayasa sosial dengan memanfaatkan data pribadi mulai terjadi, khususnya pada kasus pengambilan data pribadi nasabah perbankan melalui SMS, telepon, maupun media sosial.

2013-2017

Modus penipuan berbasis rekayasa sosial yang terjadi seperti undian berhadiah, *advance-fee scam*, peretasan email perusahaan, pemalsuan website, *phising*, dan "mama minta pulsa".

Maret 2018

Meminta kode OTP untuk transaksi finansial.

November 2018

Meminta kode verifikasi penyedia jasa telekomunikasi melalui SMS/telepon.

Februari 2019

Menghubungi pengguna *e-wallet* untuk mendapatkan kode OTP dengan kedok mendapat hadiah.

Desember 2019

Akses OTP *e-wallet* melalui *call forwarding* (kasus Maia Estianty).

November 2019

Kasus penipuan *e-wallet* Aura Kasih melalui OTP.

April 2019

Modus penipuan dengan meminta kode verifikasi aplikasi olah pesan.

Grafik 2. Perkembangan kasus penipuan dengan teknik rekayasa sosial (2013-2019).



Penipuan rekayasa sosial yang menargetkan pengguna *fintech* mulai marak di tahun 2018. Pada umumnya, penipu berusaha mendapatkan kode OTP melalui SMS maupun telepon. Beberapa kasus penipuan dilakukan menggunakan berbagai kedok, seperti undian berhadiah dan merekayasa sebuah kejadian darurat yang mengharuskan pengguna untuk memberikan data pribadi kepada pelaku.

Di akhir tahun 2019, terjadi kasus penipuan rekayasa sosial yang lebih rumit dan menjadi populer karena melibatkan Maia Estianty. Pada kasus ini, pelaku menggunakan fitur *call forwarding* untuk mendapatkan kode OTP dari Maia. Metode penipuan ini tergolong baru, karena sebelumnya pelaku hanya meyakinkan pelaku melalui SMS maupun telepon. Secara keseluruhan, walaupun terdapat perkembangan modus dan media penipuan berbasis rekayasa sosial, dapat disimpulkan bahwa: manusia atau pengguna layanan, sebagai pihak yang memiliki data adalah pihak terpenting dalam rantai keamanan siber. Beberapa contoh modus penipuan misalnya masih menyasar psikologis pengguna dengan iming hadiah maupun menempatkan mereka pada posisi darurat yang membuat mereka lengah dan memberikan data. Oleh karena itu diperlukan kompetensi spesifik terkait aspek keamanan untuk pengguna.

Edukasi untuk peningkatan kompetensi keamanan pengguna teknologi digital guna melawan penipuan berbasis rekayasa sosial: Tiga teknik kompetensi untuk menghindari penipuan dengan teknik rekayasa sosial.

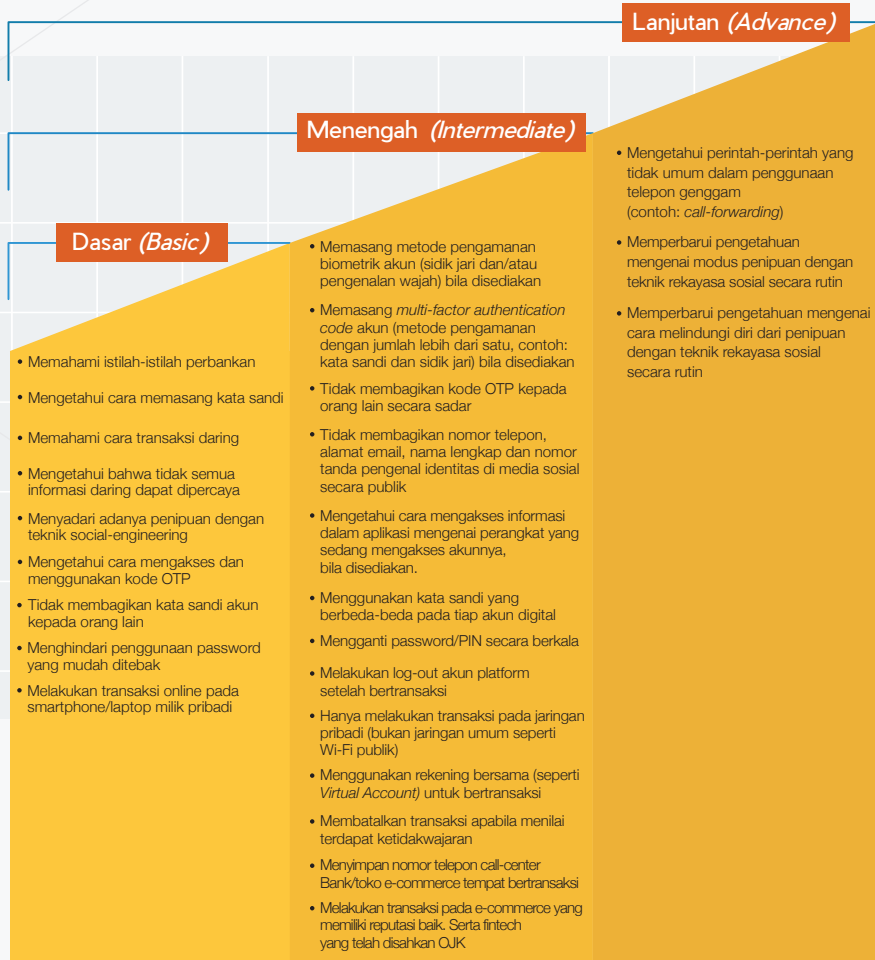




Literasi digital, terutama dalam aspek keamanan penggunaan teknologi merupakan hal utama yang menentukan ketahanan pengguna teknologi dari penipuan dengan teknik rekayasa sosial. Untuk merumuskan kompetensi dari literasi digital yang secara spesifik melindungi pengguna teknologi dari penipuan dengan teknik rekayasa sosial, kajian ini mengadopsi aspek keamanan pada *Digital Competence* (Kompetensi Digital) yang digunakan oleh Uni Eropa.³ Selanjutnya, konsep tersebut oleh penulis dikontekstualisasikan dengan kondisi penipuan dengan teknik rekayasa sosial dalam ekosistem teknologi di Indonesia

berdasarkan *global framework of reference on digital literacy skills for indicator*.⁴ Adopsi tersebut menghasilkan Kompetensi Keamanan Teknologi Digital (KKTD). Tipologi literasi pada KKTD ini dapat dikategorisasikan sebagai tiga kategori: dasar (*basic*), menengah (*intermediate*), dan lanjutan (*advanced*). Penjelasan lebih lanjut mengenai kategori adalah sebagai berikut:





Grafik 3. Kompetensi Keamanan Teknologi Digital (KKTD)





■ KOMPETENSI KEAMANAN TEKNOLOGI DIGITAL TINGKAT DASAR (*BASIC*)

Pengguna teknologi dalam tingkat *basic* memiliki KKTD dasar yang pada umumnya dimiliki seseorang ketika telah menggunakan perangkat digital dan platform teknologi. Pada tingkat ini, pengguna masih sangat rentan terhadap penipuan dengan teknik rekayasa sosial oleh karena pengguna belum mengerti risiko-risiko yang dihadapi ketika

pengguna memberlakukan fitur-fitur keamanan secara kurang bijaksana, sebagai contoh, secara sadar membagikan kode *One Time Password* (OTP), kode *Personal Identification Number* (PIN), data pribadi, atau informasi rahasia lainnya kepada orang lain.

■ KOMPETENSI KEAMANAN TEKNOLOGI DIGITAL TINGKAT MENENGAH (*INTERMEDIATE*)

Pada tingkat *intermediate*, pengguna teknologi memiliki seluruh KKTD tingkat dasar dan kompetensi tambahan yang dimiliki oleh individu yang memiliki perhatian mengenai dasar keamanan dalam bertransaksi dan membagikan data pribadi. Sebagai contoh, tidak membagikan kode OTP kepada orang lain secara sadar, menggunakan kata sandi yang berbeda-beda pada tiap akun digital, dan mengaktifkan pilihan otentikasi multifaktor pada akun digital pribadi.

Meski telah melakukan beberapa upaya penting, pengguna teknologi tingkat menengah masih cukup rentan terhadap penipuan teknologi dengan teknik rekayasa sosial, khususnya terhadap penipuan yang menggunakan perintah-perintah dalam perangkat telepon genggam yang belum diketahui secara umum, seperti memancing korban untuk memasukkan nomor telepon dengan awalan “**21*” untuk secara tidak sadar melakukan *call forwarding*.⁵





■ KOMPETENSI KEAMANAN TEKNOLOGI DIGITAL TINGKAT LANJUTAN (ADVANCED)

Terakhir, pada tingkat *advanced*, pengguna teknologi memiliki seluruh KKTD tingkat *basic* hingga *intermediate*, mengetahui perintah-perintah digital yang tidak umum, serta memiliki kompetensi untuk secara aktif memperbarui dirinya dengan informasi mengenai penipuan dengan teknik rekayasa sosial. Dengan demikian, pengguna teknologi dapat menyimpulkan strategi pertahanan diri yang diperlukan untuk menghadapi modus penipuan dengan teknik rekayasa sosial yang baru.

Berdasarkan tipologi di atas, semakin lengkap kompetensi digital yang dimiliki oleh pengguna teknologi, semakin tinggi tingkat resiliensi pengguna tersebut terhadap penipuan dengan teknik rekayasa sosial. Tipologi di atas dapat digunakan sebagai dasar bagi para pemangku kepentingan untuk merumuskan materi peningkatan literasi digital pengguna teknologi terkait keamanan informasi dan penggunaan teknologi.

■ REKOMENDASI PENCEGAHAN PENIPUAN DENGAN TEKNIK REKAYASA SOSIAL: PENDIDIKAN, PELATIHAN, DAN PENINGKATAN KESADARAN

Pendekatan yang bertujuan untuk meningkatkan ketahanan pengguna diperlukan oleh karena penipuan dengan teknik rekayasa sosial seringkali memanfaatkan kurangnya kompetensi

keamanan pengguna teknologi. Peningkatan resiliensi khususnya melalui edukasi dapat dilakukan oleh berbagai pemangku kepentingan (*multi-stakeholder*) terkait yaitu:



1

Industri
Teknologi



2

Pemerintah
dan Regulator



3

Organisasi
Masyarakat



4

Akademisi



5

Individu

Kajian ini merekomendasikan upaya yang dapat dilakukan oleh kelima pemangku kepentingan guna mencegah penipuan dengan cara meningkatkan kompetensi keamanan pengguna teknologi. Mengingat kompetensi keamanan pengguna teknologi merupakan penentu dari keberhasilan tindak penipuan tersebut, upaya pencegahan penipuan dengan teknik rekayasa sosial harus bertujuan untuk meningkatkan kompetensi keamanan pengguna teknologi. Untuk itu, pengguna teknologi yang merupakan target dari upaya tersebut harus didefinisikan terlebih dahulu.

Menurut Undang-Undang Nomor 11 Tahun 2016 tentang Informasi dan Transaksi Elektronik, pengguna teknologi dan sistem elektronik mencakup perseorangan (baik warga negara Indonesia, warga negara asing, maupun badan hukum), serta badan usaha (perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum). Oleh karena luasnya definisi pengguna teknologi, pendekatan peningkatan kompetensi keamanan pengguna teknologi harus dilakukan oleh seluruh pemangku kepentingan. Pelaksanaan peningkatan kemampuan

pengguna dalam kedua pendekatan tersebut dapat menggunakan KKTD sebagai dasar penyusunan materi peningkatan kompetensi keamanan pengguna teknologi. Meski menggunakan dasar tersebut, materi dapat disampaikan secara unik. Pemangku kepentingan juga dapat melakukan meningkatkan fitur keamanan platform teknologi untuk mengurangi risiko penipuan dengan teknik rekayasa sosial.



1 INDUSTRI TEKNOLOGI

Industri teknologi memiliki kewajiban untuk turut serta dalam peningkatan kompetensi keamanan pengguna teknologi. Kewajiban ini diatur dalam berbagai peraturan di Indonesia, diantaranya PP no. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik pasal 28, POJK no. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan pasal 14.⁶ Selain memiliki tanggung jawab untuk menjaga keamanan sistem elektronik yang digunakan dalam pelayanannya, pemain industri teknologi juga dapat mendukung peningkatan

literasi pengguna terhadap kompetensi keamanan melalui upaya sebagai berikut:

- **Menyelenggarakan kampanye anti-penipuan rekayasa sosial**

Kampanye anti-penipuan dapat dilakukan oleh industri teknologi untuk meningkatkan kesadaran publik terhadap berbagai jenis penipuan berbasis rekayasa sosial. Kampanye juga dapat digunakan untuk menambah pengetahuan serta meningkatkan kemampuan pengguna untuk dapat melindungi diri dari penipuan berbasis rekayasa sosial saat mereka



menggunakan teknologi. Kampanye anti-penipuan dapat direalisasikan misalnya dengan kampanye media sosial dan “Festival Anti-Penipuan”. Kampanye anti penipuan dapat direalisasikan, misalnya dengan kampanye di berbagai platform media sosial dengan mengajak *influencer* dan masyarakat umum untuk bergabung melawan penipuan.

- **Menyediakan fitur edukatif di dalam platform sistem elektronik**

Peningkatan kompetensi keamanan melalui platform merupakan salah satu cara yang paling efektif karena interaksi perusahaan dan pengguna teknologi mayoritas berada dalam aplikasi. Dengan menyediakan fitur di dalam platform, pengguna teknologi dapat meningkatkan kompetensi keamanan secara lebih efisien dan praktis.

Fitur dalam platform dapat didesain dengan berbagai bentuk. Salah satu contoh yang dapat dilakukan adalah mendesain sebuah permainan dalam bentuk kuis yang memungkinkan pengguna untuk merefleksikan pengetahuan mengenai penipuan dengan teknik rekayasa sosial, mengetahui apakah informasi yang diketahui sudah akurat, dan jika belum, mengetahui informasi yang akurat. Pendekatan melalui kuis ini telah digunakan oleh beberapa platform teknologi di Indonesia meskipun tidak secara langsung menasar keamanan dalam penggunaan platform teknologi. Materi yang digunakan sebagai dasar pembuatan kuis ini dapat didasarkan dengan KKTD.



● **Menyelenggarakan forum diskusi lintas industri**

Penipuan dengan teknik rekayasa sosial tidak selalu terjadi pada seluruh industri dengan metode yang sama. Oleh karena itu, forum diskusi yang memungkinkan pembagian informasi mengenai perkembangan metode penipuan dengan teknik rekayasa sosial perlu diinisiasi oleh industri teknologi ataupun asosiasi usaha terkait. Forum

antar-industri dapat diadakan secara rutin untuk saling memperbarui informasi sehingga pemain industri teknologi dapat terus memperbarui upayanya dalam mengedukasi pengguna platformnya, serta meningkatkan keamanan sistem elektroniknya jika diperlukan.



2 PEMERINTAH DAN REGULATOR

Dari segi kebijakan, pemerintah dapat terus mengedepankan kebijakan yang mengintegrasikan kompetensi keamanan teknologi digital ke dalam strategi dan kebijakan keseluruhan mengenai peningkatan kapasitas sumber daya manusia (SDM) Indonesia. Pemerintah dapat secara terus menerus menyisipkan informasi yang berkaitan dengan keamanan dalam penggunaan teknologi dalam program-program pemberdayaan masyarakat. Program ini dapat berbentuk pelatihan dengan melibatkan relawan digital di seluruh Indonesia serta memanfaatkan multi-kanal seperti media sosial dan media konvensional. Selanjutnya, materi yang bersifat panduan, seperti panduan literasi digital untuk pelaku industri dan instansi Pendidikan, atau

modul pelatihan peningkatan keamanan pengguna teknologi, dapat menjadi acuan yang efektif bagi seluruh pemangku kepentingan dalam upaya Bersama melawan penipuan berbasis rekayasa sosial. Kolaborasi multi-pihak antara pemerintah dengan pelaku industri dapat terus berlanjut untuk memastikan agar upaya edukasi pengguna teknologi tentang pentingnya menjaga keamanan informasi dan untuk waspada terhadap penipuan berbasis rekayasa sosial dapat menjangkau masyarakat yang lebih luas. Kolaborasi tersebut juga dapat memberikan insentif kepada pelaku industri untuk dapat meningkatkan transparansi serta mengedukasi penggunanya mengenai teknologi terbaru atau fitur keamanan yang dimiliki oleh suatu platform.⁷



3

ORGANISASI MASYARAKAT

Peran organisasi masyarakat dalam pendekatan ini adalah untuk menyebarkan informasi mengenai perilaku penggunaan teknologi yang aman, berdasarkan KKTD. Organisasi masyarakat yang dapat berkontribusi dalam pendekatan ini meliputi organisasi masyarakat yang bergerak dalam bidang literasi digital (sebagai contoh: Siberkreasi, ICT Watch, Relawan TIK Indonesia), keamanan data pribadi (sebagai contoh: SAFEnet dan ELSAM), PARFI, IGF Indonesia, Jaringan Pegiat Literasi Digital Indonesia, Siberkreasi maupun Lembaga keamanan konsumen (sebagai contoh: YLKI). Upaya-upaya yang dapat dilakukan oleh organisasi masyarakat dalam pendekatan ini adalah sebagai berikut:

Tujuan Kegiatan	Inisiatif yang dapat dilakukan
Meningkatkan kesadaran masyarakat mengenai keamanan dalam menggunakan teknologi.	Menyisipkan materi peningkatan kompetensi keamanan dalam program penyuluhan literasi digital.
	Menyusun buku acuan yang bertujuan untuk meningkatkan kompetensi keamanan, yang dapat digunakan sebagai rujukan oleh lembaga pendidikan untuk melakukan peningkatan kompetensi keamanan.
Mengevaluasi dan memberi masukan terkait kebijakan pemerintah dan regulator maupun industri teknologi yang berkaitan dengan keamanan dalam penggunaan teknologi	Mengevaluasi dan memberi masukan program atau pendekatan yang dilakukan oleh pemerintah dan regulator dalam meningkatkan kompetensi keamanan.
	Mengevaluasi dan memberi masukan terhadap inisiatif yang dilakukan oleh industri teknologi dalam meningkatkan kompetensi keamanan.

Tabel 1. Upaya yang dapat dilakukan oleh Organisasi Masyarakat.



4 AKADEMISI

Peran utama akademisi dalam pendekatan ini adalah untuk meneliti upaya peningkatan kompetensi keamanan oleh berbagai pemangku kepentingan dan memberikan inovasi terhadap upaya peningkatan tersebut. Kajian mengenai penipuan dengan teknik rekayasa sosial di Indonesia masih belum cukup. Padahal, Indonesia memiliki akademisi dan lembaga penelitian yang bergerak dalam penelitian di bidang isu-isu digital, seperti: Center for Digital Society (CfDS) UGM, Cyber Law Center UNPAD, Swiss German University - Cyber Security Laboratory, Binus University - Cyber Security Program dan lainnya. Dengan demikian, di antara permasalahan terkait penipuan dengan teknik rekayasa sosial yang dapat diteliti, akademisi-akademisi tersebut dapat melakukan penelitian yang mencoba mencakup isu-isu berikut ini:

- **Kritik terhadap kompetensi dasar terkait resiliensi terhadap penipuan dengan teknik rekayasa sosial**

Saat ini, belum terdapat studi yang merumuskan kompetensi dasar yang dibutuhkan oleh pengguna teknologi untuk meningkatkan resiliensi terhadap penipuan dengan teknik rekayasa sosial. Meski demikian, KKTD yang disusun dalam kajian ini harus diperbarui dan dilengkapi apabila terdapat perkembangan dalam kasus-kasus penipuan dengan teknik rekayasa sosial di masa depan yang memanfaatkan fitur-fitur keamanan maupun kebiasaan digital masyarakat yang baru. Untuk itu, penelitian yang ditujukan untuk memperbarui kompetensi keamanan menjadi penting untuk dilakukan.



- **Penelitian tentang jumlah dan persebaran pengguna teknologi informasi dan komunikasi berdasarkan tingkat kompetensi keamanannya**

Penipuan dengan teknik rekayasa sosial seringkali menasar pengguna teknologi informasi dan komunikasi. Berdasarkan tinjauan pustaka, penelitian mengenai jumlah dan persebaran pengguna teknologi informasi dan komunikasi berdasarkan tingkat kompetensi keamanannya belum pernah dipublikasikan. Padahal, mengetahui jumlah pengguna teknologi informasi dan komunikasi berdasarkan tingkat kompetensi keamanannya dapat membantu pemangku kepentingan, utamanya pemerintah dan regulator dan industri teknologi, untuk merumuskan dan melaksanakan kebijakan dan inisiatif yang sesuai dengan kebutuhan pengguna pada tingkat kompetensi keamanan tertentu. Terlebih, masih belum ada penelitian yang dipublikasikan mengenai tren penipuan rekayasa sosial di Indonesia, tipologi pelaku dan korban, serta persebaran korban dan kejadian. Oleh sebab itu, pertanyaan penelitian ini perlu diupayakan untuk dijawab oleh akademisi.

- **Evaluasi berbagai kebijakan dan inisiatif pencegahan penipuan dengan teknik rekayasa sosial**

Pendekatan yang saat ini digunakan oleh pemerintah dan yang direkomendasikan dalam penelitian ini adalah pendekatan yang ditujukan untuk meningkatkan kompetensi keamanan pengguna teknologi guna meningkatkan resiliensinya terhadap penipuan dengan teknik rekayasa sosial. Namun demikian, efektivitas upaya yang dilakukan dalam kedua pendekatan ini perlu dievaluasi secara lebih lanjut melalui penelitian lanjutan.





- **Pengembangan pendekatan inovatif dalam meningkatkan kompetensi keamanan pengguna teknologi**

Pendekatan yang lebih inovatif untuk meningkatkan kompetensi keamanan pengguna teknologi berpotensi meningkatkan efektivitas proses edukasi kompetensi keamanan tersebut. Menurut Khan dkk., pendekatan ini sudah diusulkan oleh beberapa peneliti keamanan informasi seperti Newfound dan Furnell⁸, serta Cone dkk.⁹ Pendekatan seperti ini telah dicoba oleh

oleh DROG¹⁰, sebuah kelompok multidisipliner yang berkantor di Den Haag, untuk menangani penyebaran *information disorder*. Online game yang dinamai sebagai Bad News Game ini didesain untuk memberikan pemain perspektif sebagai pembuat berita bohong agar tidak ikut menyebarkan berita bohong.¹¹ Meski inovatif, pendekatan seperti ini bersifat eksperimental dan membutuhkan biaya yang besar, maka pendekatan ini sebaiknya dilakukan secara kolaboratif bersama pemangku kebijakan lain, seperti industri teknologi.



5 INDIVIDU

Individu yang merupakan pengguna maupun calon pengguna teknologi dapat berupaya aktif untuk meningkatkan kompetensi keamanannya. Pada dasarnya, pengguna juga bertanggung jawab untuk menjaga kerahasiaan data pribadi dan memastikan keamanan informasi rahasia lainnya. Pada gambar 2, individu diharapkan dapat memenuhi kompetensi yang tertuang dalam KKTD tersebut. Melihat kasus-kasus penipuan dengan teknik rekayasa sosial yang terjadi di Indonesia, mayoritas pengguna teknologi berada pada tingkat *basic* dan



intermediate. Untuk itu, pengguna teknologi Indonesia dapat berupaya aktif meningkatkan kompetensinya dengan selalu memperbaharui pengetahuannya mengenai teknologi di sekitarnya dan bagaimana cara untuk menggunakan teknologi tersebut.

Bagi pengguna teknologi yang berada pada tingkat *basic*, pengguna harus mulai membiasakan diri untuk melakukan kompetensi yang terdapat pada tingkat *intermediate* dengan cara: membuat pengingat di telepon genggam secara berkala (sebagai contoh setiap tiga bulan sekali) untuk mengganti *password* yang pada tiap akun digital, mematikan akses telepon genggam ke WIFI publik apabila hendak menggunakan aplikasi perbankan digital, meneliti terlebih dahulu reputasi platform *e-commerce* yang digunakan maupun penjual dalam

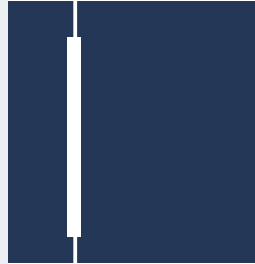
e-commerce sebelum bertransaksi dengan platform maupun penjual tersebut dan membiasakan diri untuk menggunakan akses keamanan lebih dari satu (sebagai contoh *password* dan sidik jari).

Bagi pengguna teknologi yang berada pada tingkat *intermediate*, pengguna harus mulai melatih diri untuk lebih proaktif dalam melindungi diri saat menggunakan teknologi dengan cara: mengikuti berita/media yang membahas mengenai kasus keamanan siber, mencari dan berupaya mengerti secara seksama metode-metode baru yang digunakan oleh pelaku penipuan dan mempelajari perintah/fitur teknologi yang tidak diketahui secara umum, namun dapat dimanfaatkan oleh pelaku penipuan untuk melaksanakan penipuan berbasis rekayasa sosial.



■ KESIMPULAN

Penipuan dengan teknik rekayasa sosial adalah penipuan yang dilakukan dengan cara manipulasi psikologis korban, bukanlah manipulasi sistem atau peretasan sistem. Penipuan berbasis rekayasa sosial bisa terjadi karena penipu memanfaatkan rendahnya pengetahuan serta kompetensi pengguna teknologi mengenai keamanan digital. Kajian ini mengidentifikasi bahwa modus penipuan dengan teknik rekayasa sosial menysasar berbagai sektor di industri teknologi, informasi, dan komunikasi (TIK) di Indonesia. Perumusan tipologi pengguna berdasarkan kompetensi keamanan yang dimiliki telah dirancang, dan menemukan bahwa pemahaman para pengguna teknologi di Indonesia tentang keamanan digital masih berada pada tingkat dasar dan menengah. Selanjutnya, karena penipuan dengan rekayasa sosial terjadi di berbagai sektor, rekomendasi untuk mengedukasi pengguna teknologi akan kompetensi keamanan digital menjadi peran dan tanggung jawab seluruh pemangku kepentingan terkait. Oleh karena itu, untuk mencegah penipuan berbasis rekayasa sosial, kajian ini merekomendasikan upaya edukasi peningkatan kompetensi keamanan pengguna teknologi.



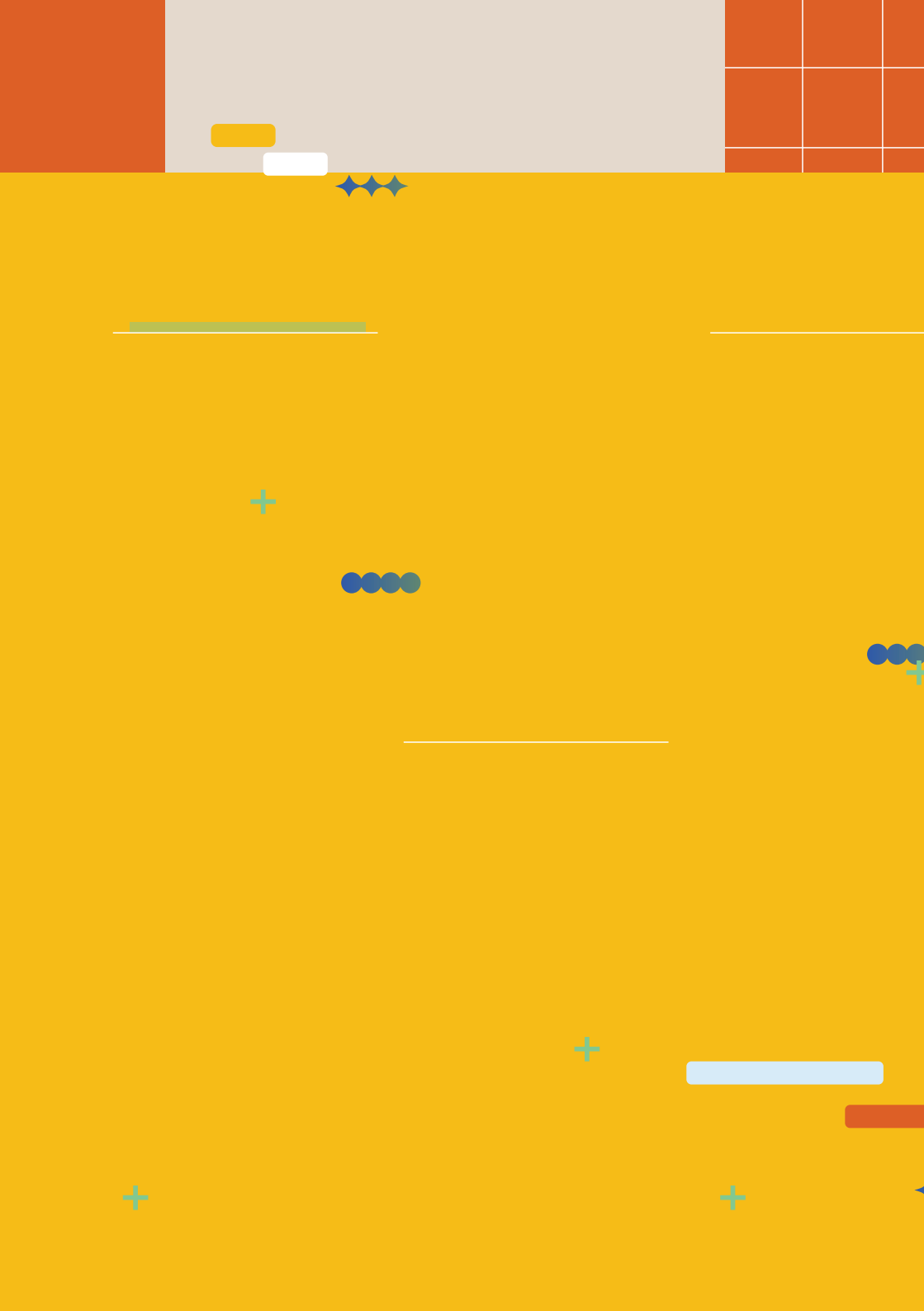
REFERENSI

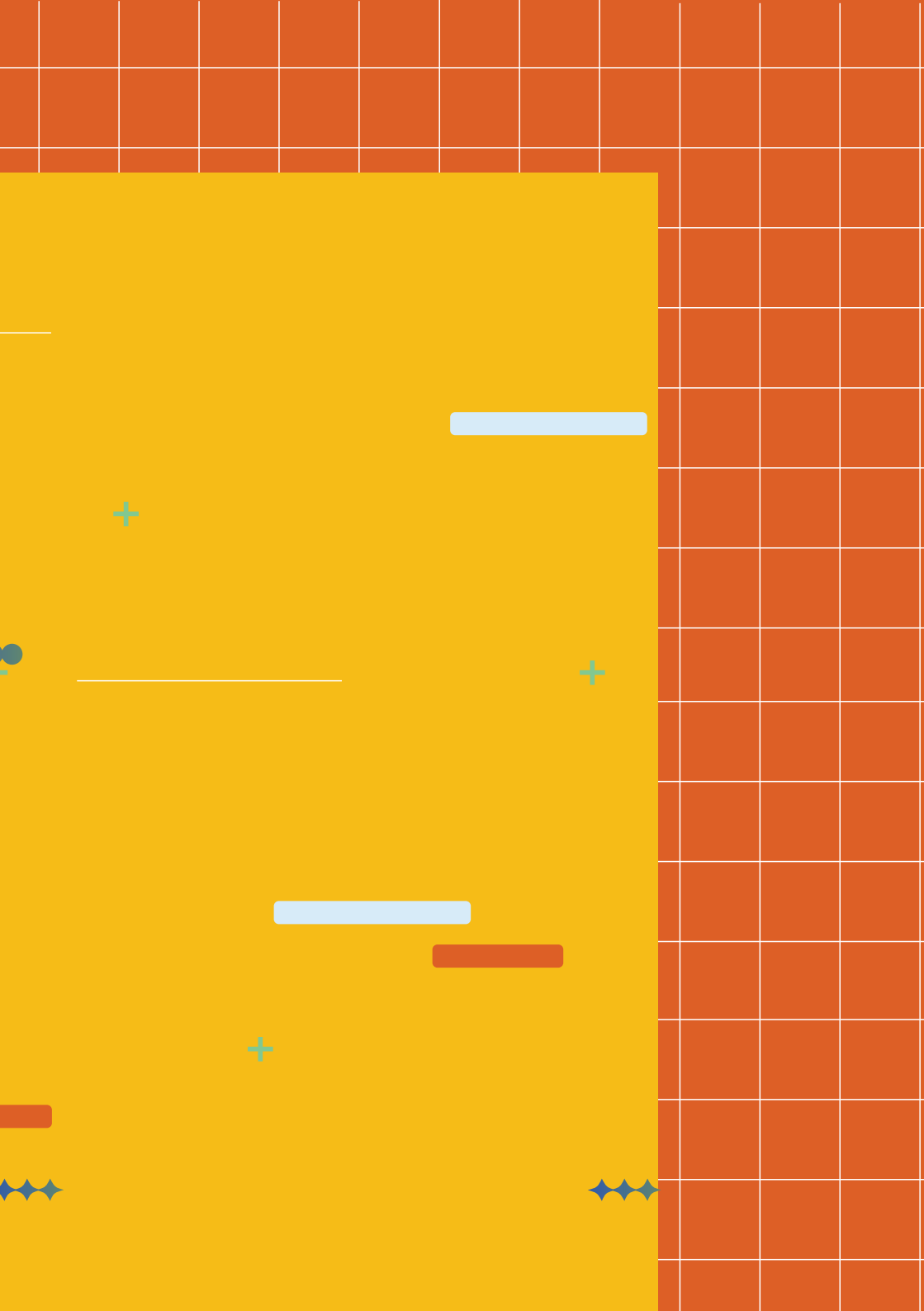
- ¹Chubb. (2018). Combating Social Engineering Fraud: A Guide for Chubb Insureds. [daring] Chubb.com. Tersedia di https://www.chubb.com/us-en/_assets/doc/14-01-1279-guide-to-combating-sef-08.18.pdf [Diakses pada 30 Januari 2020].
- ²Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*. Vol. 59. hal. 186-209.
- ³Lebih lanjut mengenai Digital Competence Europass, lihat Europass. (n.d.). Digital competence. [daring] Tersedia di <https://europass.cedefop.europa.eu/resources/digital-competences>. [Diakses pada 20 Januari 2020].
- ⁴Law, N., Woo, D., de la Torre, J., & Wong, G. (2018). A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4. 2, Information Paper No. 51. Montreal: UNESCO Institute for Statistics.
- ⁵Lebih lanjut mengenai berita penipuan yang memanfaatkan call-forwarding, lihat Kumparan. (2019). Kata Telkomsel Soal Call Forward di Penipuan Akun Gojek Maia Estianty. [daring] Tersedia di <https://kumparan.com/kumparantech/kata-telkomsel-soal-call-forward-di-penipuan-akun-gojek-maia-estianty-1sWljSJM5rP>. [Diakses pada 20 Januari 2020].
- ⁶Peraturan Otoritas Jasa Keuangan Nasional nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, pasal 14.
- ⁷World Economic Forum (WEF). (2016). Shaping the Future Implications of Digital Media for Society Improving End User Digital Media Literacy. [daring] Tersedia di: http://www3.weforum.org/docs/WEF_Meeting_Improving_End_User_Digital_Media%20Literacy.pdf. [Diakses pada 20 Januari 2020]
- ⁸Newbould, M. dan Furnell, S. (2009). Playing Safe: A Prototype Game For Raising Awareness of Social Engineering. In: The 7th Australian Information Security Management Conference. [daring] Perth: ECU, hal. 24-30. Tersedia di: <https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1003&context=ism>. [Diakses pada 21 Januari 2020].
- ⁹Cone, B. D., Thompson, M. F., Irvine, C.E., dan Nguyen, T. D. (2011). Cyber Security Training and Awareness Through Game Play. In:

Fischer-Hübner S., Rannenberg K., Yngström L., Lindskog S. (eds) Security and Privacy in Dynamic Environments. SEC 2006. IFIP International Federation for Information Processing. Vol 201. Tersedia di: https://link.springer.com/chapter/10.1007/0-387-33406-8_37.

¹⁰DROG. (n.d.) A Good Way to Fight Bad News. [daring]. Tersedia di: <https://www.aboutbadnews.com/>. [Diakses pada 21 Januari 2020]

¹¹Bad News Game. (n.d.) How Does Bad News Work?. [daring]. Tersedia di: <https://getbadnews.com/#intro>. [Diakses pada 21 Januari 2020]





ABOUT CFDS

Center for Digital Society (CfDS) is the research center established by the Faculty of Social and Political Sciences, Universitas Gadjah Mada. The institution is created under the concern over the contemporary dynamics of socio-political condition of the world that is accentuated by the impeccable influence of information technology. The phenomenon triggers the new patterns and complexities in the society, and thus requires new approaches in managing such complexities.

CfDS pledged to delve more on the study of contemporary digital society, including related issues surrounding the topic; such as the issues of smart city and urban development. The emphasis is then put on the utilization of technology to shape the society in becoming digitalized, as well as to bring solvency to social issues.

Vision

Solving Social Problem and Accelerating Prosperity through Indonesia Digital Society

Activities

1. Research and Development
2. Dissemination and Publication
3. Education and Policy Advocacy

Research Scopes

1. Digital Governance
2. Digital Economy
3. Future Technology



facebook.com/cfdsugm



@cfds_ugm



Center for Digital Society (CfDS)



@cfds_ugm



cfds.fisipol.ugm.ac.id



cfds_ugm



CFDS UGM