CfDS CENTER FOR DIGITAL SOCIETY
UNIVERSITAS GADJAH MADA
gojek
gopay

Kajian Peningkatan Kompetensi Keamanan Digital di Indonesia:

Analisis Fenomena Penipuan dengan Teknik Rekayasa Sosial

Center for Digital Society
Universitas Gadjah Mada
2020

Kajian ini dirumuskan oleh Center for Digital Society (CfDS), pusat studi yang didirikan oleh Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Gadjah Mada. Institusi ini didirikan atas dasar perkembangan dan dinamika kehidupan sosial-politik kontemporer di dunia, yang ditandai dengan pengaruh dari teknologi informasi. Kajian ini disusun dengan dukungan dari Gojek dan GoPay.

Penulis:
Anaq Duanaiko
Janitra Haryanto
Paska Bayu Darmawan
Yuliana Khong

Editor:
Anisa Pratita Kirana Mantovani

Desain dan Tata Letak:
Masgustian
Naufal Alatas Radityasakti

Daftar Isi

Ringkasan Eksekutif

1. Fenomena penipuan dengan teknik rekayasa sosial, atau yang juga dikenal sebagai manipulasi psikologis, saat ini marak terjadi di Indonesia dan mendapatkan perhatian penuh dari berbagai industri di Indonesia.

2. Hal ini disebabkan oleh pemanfaatan teknologi masyarakat Indonesia yang tidak sebanding dengan tingkat literasi digital masyarakat yang masih tergolong rendah, utamanya mengenai keamanan dalam penggunaan teknologi. Kesenjangan tersebut menjadi salah satu penyebab utama maraknya penipuan dengan teknik rekayasa sosial yang memanfaatkan lengahnya pengguna teknologi akan menjaga keamanan informasi pribadi miliknya. Sehingga, pelaku penipuan dapat melakukan serangan tanpa harus meretas keamanan sistem elektronik yang digunakan.

3. Kajian ini menemukan bahwa penipuan dengan teknik rekayasa sosial dapat dicegah dengan, salah satunya, mengedukasi pengguna dan calon pengguna teknologi guna meningkatkan literasi digital, atau yang kemudian disebut dengan Kompetensi Keamanan Teknologi Digital (KKTD). Peningkatan KKTD dapat dicapai dengan cara pendidikan, pelatihan, dan peningkatan kesadaran pengguna.

4. Kajian ini juga menemukan bahwa peningkatan literasi digital atau KKTD pengguna teknologi di Indonesia menjadi tanggung jawab bersama para pemangku kepentingan, yang diidentifikasi sebagai pemerintah, industri, organisasi masyarakat, dan pengguna itu sendiri.


gopay
gopay

Pendahuluan

Perkembangan teknologi telah memungkinkan berbagai negara untuk mengembangkan potensi ekonomi digitalnya secara masif. Indonesia adalah salah satu negara dengan potensi ekonomi digital yang menjanjikan. Laporan yang dipublikasikan oleh McKinsey menyebutkan pada tahun 2025, perekonomian digital Indonesia diperkirakan akan mencapai USD 150 miliar.[1] Kenaikan tersebut juga diprediksikan di dalam laporan yang dipublikasikan oleh Google, Temasek, dan Bain & Co (USD 130 Miliar) karena adanya adopsi penggunaan pembayaran digital oleh

1. Das, K., Gryseels, M., Sudhir, P. and Tan, K. (2020) Unlocking Indonesia's digital opportunity. [daring] Mckinsey.com. Tersedia di: https://www.mckinsey.com/~/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx. [Diakses pada 30 Jan 2020].

semua sektor.[2] Meski demikian, perkembangan potensi ekonomi digital berkembang seiring dengan potensi kejahatannya. Consultative Group to Assist the Poor (CGAP) menunjukkan bahwa 83% dari sampel penelitiannya di Filipina merupakan target penipuan berbasis telepon genggam, dimana 17% dari sampel tersebut kehilangan uang dari penipuan tersebut. Lebih lanjut, 27% dari sampel penelitian CGAP di Tanzania merupakan target penipuan dan 17% dari sampel penelitian tersebut merugi.[3] Kasus-kasus penipuan berbasis telepon genggam juga terjadi di Indonesia. Kasus ini seringkali dikenal sebagai penipuan dengan teknik rekayasa sosial.

Penipuan dengan teknik rekayasa sosial dilakukan dengan menembus jaringan keamanan melalui manipulasi pengguna untuk mendapatkan informasi rahasia.[4] Secara umum, teknik ini memanfaatkan psikologi korban dan menargetkan pengguna yang tidak memahami pentingnya melindungi data pribadi dan menjaga keamanan informasi rahasia lainnya.[5] Meski tidak menggunakan kemampuan teknik yang kuat, penipuan dengan teknik rekayasa sosial terjadi pada berbagai industri teknologi, informasi dan komunikasi di Indonesia.[6]

Menanggapi hal tersebut, peningkatan literasi digital pengguna dan kerjasama berbagai pemangku kepentingan menjadi hal yang fundamental. Masyarakat sebagai pengguna teknologi diharuskan memiliki kompetensi keamanan digital yang cukup. Sementara pihak pemerintah dan pelaku industri dapat bekerja sama untuk menciptakan ekosistem digital yang aman dan inklusif. Kajian ini disusun untuk memetakan jenis penipuan dengan teknik rekayasa sosial yang terjadi di industri teknologi informasi dan komunikasi di Indonesia, serta memberikan panduan dan rekomendasi yang dapat diupayakan oleh para pemangku kepentingan yaitu: pelaku industri, pemerintah dan regulator, akademisi, organisasi masyarakat, dan para individu pengguna teknologi.

---

[2] Google, Temasek, & Bain & Company. (2019). E-conomy SEA 2019. [daring] Think Google. Tersedia di: https://www.thinkwithgoogle.com/intl/en-apac/tools-resources/research-studies/e-conomy-sea-2019-swipe-up-and-to-the-right-southeast-asias-100-billion-internet-economy/. [Diakses pada 07 Jan 2019]

[3] The Economist. (2020). How digital financial services can prey upon the poor. [daring] Tersedia di: https://www.economist.com/finance-and-economics/2020/01/30/how-digital-financial-services-can-prey-upon-the-poor [Diakses 11 Feb. 2020].

[4] Allsopp, W. (2009). Unauthorized Access: Physical Penetration Testing for IT Security Teams. West Sussex: John Wiley & Sons.

[5] Mitnick, K. and Simon, W. (2006), The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing.

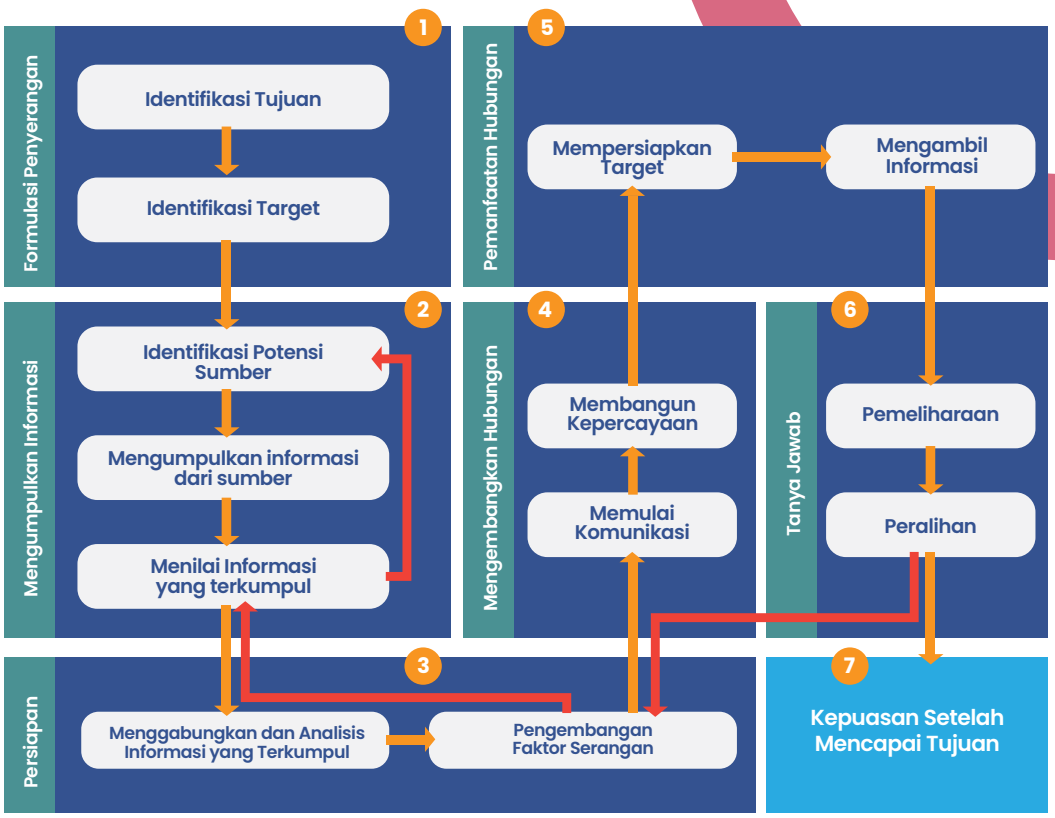
[6] Lebih lanjut mengenai industri teknologi yang terdampak oleh penipuan dengan teknik rekayasa sosial, lihat hal.4.

Fenomena penipuan dengan teknik rekayasa sosial di Indonesia

Apakah yang dimaksud dengan penipuan dengan teknik rekayasa sosial?

Penipuan dengan teknik rekayasa sosial adalah penipuan yang menggunakan kemampuan pelaku penipuan untuk membangun kepercayaan korban dan memanfaatkan kepercayaan tersebut untuk melaksanakan serangan penipuannya.[7] Dengan demikian, penipuan dengan 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.

[7] Chubb. (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 Jan 2020].



Gambar 1 . Kerangka penyerangan penipuan dengan rekayasa sosial.[8]

Melihat dari kerangka penyerangan penipuan di atas, formulasi penyerangan merupakan langkah pertama penyerangan dengan melakukan identifikasi tujuan penyerangan dan identifikasi 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 di formulasikan di awal. Ketiga, pelaku penyerangan akan melakukan persiapan dengan menggabungkan dan analisis informasi yang telah terkumpul, lalu mengembangkan faktor serangan, namun pelaku akan terus mengumpulkan informasi hingga pengembangan faktor serangan sudah dikiranya siap. 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 kepuasan dalam mencapai tujuan yang telah diformulasikan di awal.

[8] Mouton, F., Leenen, L., & Venter, H. S. (2016), Social engineering attack examples, templates and scenarios. Computers & Security, vol. 59, hal. 186-209.

Perkembangan kasus penipuan dengan teknik rekayasa sosial

Metode yang digunakan untuk mencari data mengenai tren penipuan dengan teknik rekayasa sosial, 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 berita online yang dilakukan dari tahun 2013 hingga akhir tahun 2019, 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.

Gambar 2 . Perkembangan kasus penipuan dengan teknik rekayasa sosial (2013-2019).[8]

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* (sindikat *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 menyasar perempuan di sebuah media jejaring sosial ditambah dengan kasus pembobolan internet banking dengan modus kartu sim rusak. Sedangkan pada tahun 2017, kasus rekayasa

rekayasa sosial dengan memanfaatkan data pribadi mulai terjadi, khususnya pada kasus pengambilan data pribadi nasabah perbankan melalui SMS, telepon, maupun media sosial.

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 maupun kejadian darurat yang mengharuskan pengguna untuk memberikan data pribadi kepada pelaku yang bersembunyi dibalik identitas pengemudi online ataupun kerabat dekat. Di akhir tahun 2019, terjadi kasus penipuan rekayasa sosial yang lebih *advanced* melibatkan Maia Estianty.[9] Di 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.

Apa saja karakteristik penipuan dengan teknik rekayasa sosial?

Berdasarkan pemaparan di atas, dapat disimpulkan bahwa, setidaknya, terdapat tiga karakteristik utama penipuan dengan teknik rekayasa sosial, yaitu:

A. Kepercayaan Korban: kunci keberhasilan penipuan dengan teknik rekayasa sosial

Kepercayaan korban adalah salah satu faktor di balik keberhasilan penipuan berbasis rekayasa sosial. Sebagaimana dijelaskan sebelumnya, penipuan dengan teknik rekayasa sosial menggunakan informasi pribadi dari para korban. Oleh karena itu, pelaku penipuan dengan teknik rekayasa sosial menghabiskan banyak waktu untuk mengembangkan hubungan dengan korban hingga mendapatkan kepercayaan korban. Menurut konsultan keamanan Kevin Mitnik, penipu selalu mengantisipasi kecurigaan dan kekhawatiran, serta memiliki strategi untuk mengubah ketidakpercayaan menjadi kepercayaan.[10] Dalam diskursus akademik, kemampuan ini seringkali disebut sebagai *social psychology* (psikologi sosial).

9. Lihat Lampiran.
10. Lebih lanjut mengenai faktor psikologis penipuan dengan teknik rekayasa sosial, lihat Chubb, (2018).

Jonathan J. Rusch mengidentifikasi tiga askpek psikologi sosial yang dapat digunakan oleh penipu dengan teknik rekayasa sosial[11]:

1. Alur Berpikir

Terdapat dua alur berpikir yang diterapkan dalam strategi penipu dengan teknik rekayasa sosial, yakni alur utama yang memerlukan penalaran yang logis dan alur sampingan yang memanfaatkan heuristik kemampuan penalaran.[12]

2. Sikap dan kepercayaan

Terdapat perbedaan sikap dan kepercayaan antara penipu dengan pengguna teknologi. Pengguna teknologi yang sejak awal telah memiliki sikap yang kurang berhati-hati dan tidak mencermati pesan ajakan dari seseorang, akan lebih rentan untuk dimanfaatkan oleh penipu dalam melancarkan serangannya. Ketidakcermatan ini biasanya menimbulkan kesan yang terlalu positif terhadap penipu, sehingga persepsi yang muncul terhadap penipu adalah sebagai orang yang jujur dan tidak berencana buruk.[13]

3. Teknik ajakan dan pengaruh

Teknik ajakan dan pengaruh merupakan pemanfaatan dari alur berpikir sampingan. Merangkum argumen Rusch, setidaknya terdapat enam aspek yang dapat mempengaruhi kepercayaan orang, terlepas dari penalaran yang logis:

a. **Wewenang,** dimana penipu memainkan perannya sebagai pihak yang dianggap memiliki wewenang atau kredibilitas untuk mendorong pengguna teknologi melakukan sesuatu, pengguna menuruti perintahnya.[14]

b. **Kelangkaan,** dimana kesempatan (seperti hadiah, uang, dll.) yang ditawarkan oleh penipu dibingkai sebagai sesuatu yang tidak selalu ada, kemungkinan pengguna untuk mengikuti permintaan penipu menjadi lebih tinggi.[15]

---

11. Rusch, J. J. (1999). The "Social Engineering" of Internet Fraud. Pada: Internet Society Annual Conference 1999. Tersedia di https://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm. [Diakses pada 3 Feb 2020].
12. Ibid.
13. Ibid.
14. Penunjukkan wewenang seringkali ditemukan pada kasus-kasus penipuan perbankan konvensional maupun teknologi, dimana pelaku berpura-pura sebagai karyawan perbankan atau perusahaan teknologi yang memiliki wewenang atas akun/objek yang dimiliki korban.
15. Strategi yang mengandung kelangkaan ini seringkali ditemukan pada kasus-kasus penipuan industri telekomunikasi dll., dimana korban ditawarkan dengan hadiah/penghargaan yang harus segera dikonfirmasi pada saat itu juga.

c. **Kesukaan dan kesamaan,** dimana penipu berhasil membingkai diri memiliki kesamaan latar belakang serta kesukaan dengan pengguna teknologi, kemungkinan pengguna secara heuristik menganggap penipu adalah orang baik menjadi meningkat.

d. **Timbal Balik,** dimana penipu berhasil membingkai pengguna teknologi sebagai orang yang memiliki hutang maupun hutang budi kepada penipu, maka pengguna memiliki beban moral untuk mengembalikan hutang tersebut dengan cara menuruti permintaan penipu.[16]

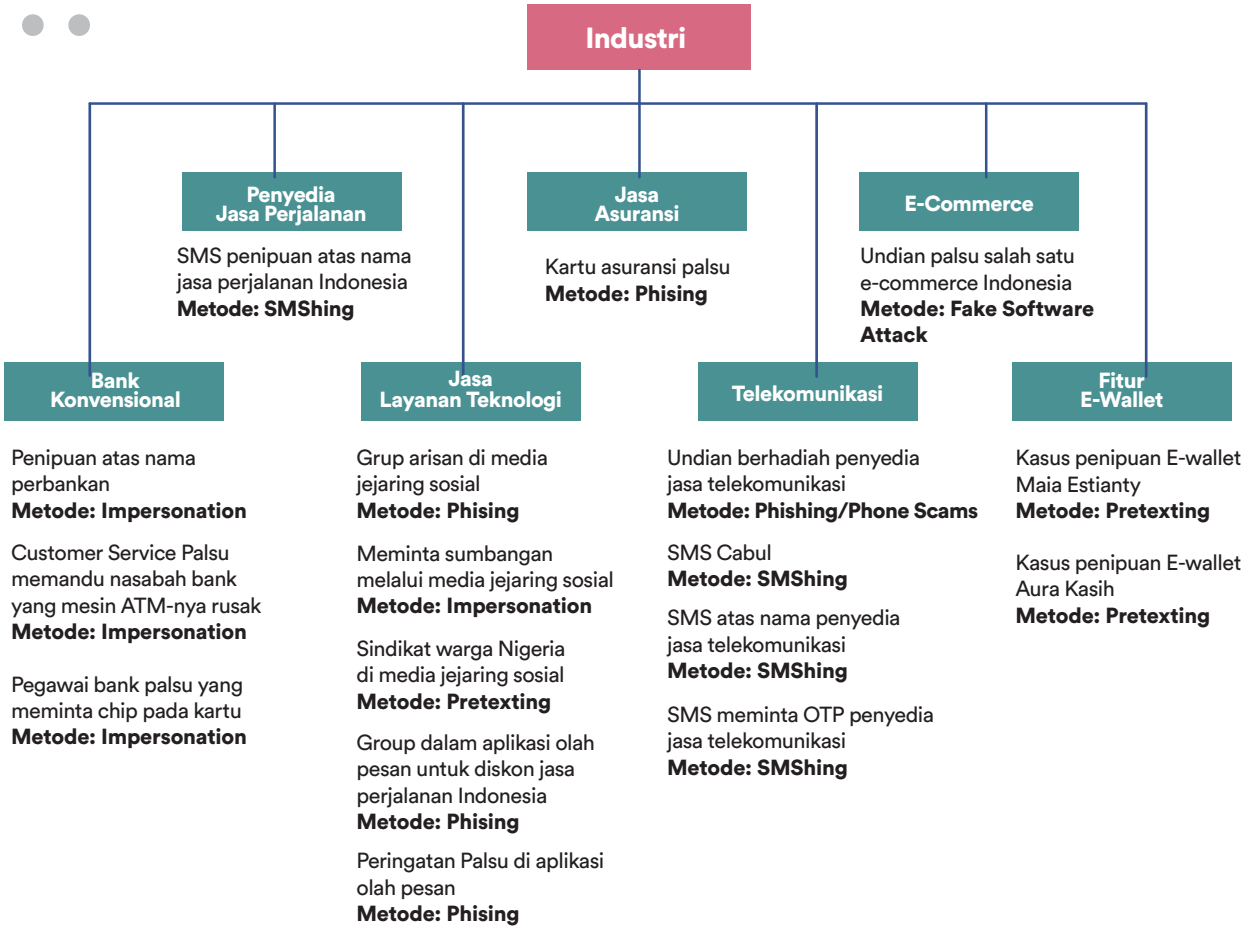
e. **Komitmen dan konsistensi,** dimana penipu menunjukkan komitmen dan konsistensi dalam detil metodenya (sebagai contoh: pesan yang dituliskan secara formal dari awal pesan hingga akhir) maka kemungkinan kepercayaan pengguna teknologi akan meningkat.[17]

f. **Bukti sosial,** dimana lingkungan sekitar pengguna teknologi mengambil tindakan tertentu yang mendukung keberhasilan penipuan dengan teknik rekayasa sosial, maka pengguna teknologi kemungkinan besar akan melakukan hal yang sama.[18]

B. Mencakup multi-industri, menggunakan multi-metode

Dalam perkembangannya, pelaku penipuan dengan teknik rekayasa sosial mengembangkan berbagai metode penipuan sesuai dengan fitur teknologi yang berkembang dalam kehidupan sehari-hari. Melihat dari kasus penipuan dengan teknik rekayasa sosial yang telah dikumpulkan oleh penulis,[19] penipuan menyerang berbagai macam industri dengan metode yang berbeda termasuk industri bank konvensional, telekomunikasi, *e-commerce, e-wallet*, asuransi, dan lainnya. Penipuan dengan teknik rekayasa sosial menyadarkan bahwa keamanan sistem teknologi tidak cukup apabila pengguna masih belum memahami dan mencegah penipuan dengan teknik rekayasa sosial.

[16] Kasus-kasus seperti ini dapat ditemukan pada kasus "Mama Minta Pulsa" dimana pengguna teknologi digiring untuk mempersepsikan penipu sebagai ibunya, yang tentu memiliki peran yang besar dalam hidupnya.
[17] Strategi menggunakan komitmen terhadap korban seringkali terlihat pada kasus-kasus penipuan perbankan konvensional, dimana pelaku secara konsisten menyuruh korban untuk mengirimkan sejumlah uang ke rekening pelaku.
[18] Sebagai contoh, apabila lingkungan sekitar pengguna teknologi memberikan data pribadinya kepada orang lain secara mudah, maka kemungkinan pengguna teknologi tersebut akan menoleransi perilaku yang sama.
[19] Lihat Lampiran untuk melihat kasus lebih lanjut.



Gambar 3 . Jenis-jenis penipuan dengan teknik rekayasa sosial[20 21]

- *Impersonation:* Pelaku menyamar menjadi seseorang untuk mengumpulkan informasi
- *Phishing:* Pelaku mengumpulkan informasi melalui telefon, e-mail, atau media lain
- *Pretexting:* Pelaku membangun skenario yang meyakinkan untuk mengambil informasi
- *SMShing:* Sama seperti phishing, namun menggunakan SMS

C. Pencegahan merupakan tanggung jawab bersama

Penipuan dengan teknik rekayasa sosial menggunakan metode yang beragam serta menyasar berbagai industri. Hal ini menunjukkan bahwa pelaku penipuan akan selalu memperbarui metode penipuan dan juga mereplikasi metode yang berhasil pada satu industri ke industri lain. Kasus penipuan dengan teknik rekayasa sosial menjadi isu yang kompleks dan memiliki potensi target yang luas. Indonesia sebagai negara dengan penduduk yang sebagian besar masyarakatnya sudah memiliki akses kepada teknologi, namun tidak memiliki literasi digital yang cukup menjadi sasaran bagi para penipu yang menggunakan teknik rekayasa sosial.[22] Dengan demikian, pencegahan penipuan dengan teknik rekayasa sosial sebaiknya tidak dilaksanakan oleh satu pihak saja, melainkan berbagai pemangku kepentingan terkait.

[20] Ibid.
[21] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.
[22] Jurriëns, E., & Tapsell, R. (Eds.). (2017). Digital Indonesia: connectivity and divergence. ISEAS-Yusof Ishak Institute.

Edukasi untuk peningkatan Kompetensi Keamanan Pengguna Teknologi Digital guna melawan penipuan berbasis rekayasa sosial

Tiga tingkat kompetensi untuk menghindari penipuan dengan teknik rekayasa sosial

Literasi digital, terutama dalam aspek keamanan penggunaan teknologi merupakan hal utama yang berpengaruh terhadap 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.[23] 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*.[24] 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:

[23] Lebih 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 Jan 2020].
[24] Law, 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.

Gambar 4 . Kompetensi Keamanan Teknologi Digital (KKTD) (diolah oleh penulis)

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*.[25]

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.

[25] Lebih 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 Jan 2020].

Kompetensi Keamanan pengguna teknologi di Indonesia berada di tingkat basic hingga intermediate

Melihat dari kasus penipuan dengan teknik rekayasa sosial yang telah dikumpulkan penulis[26] dan mengacu pada kompetensi yang tertera dalam KKTD, dapat disimpulkan bahwa pengguna teknologi di Indonesia masih berada pada tingkat kompetensi *basic* hingga *intermediate*. Pasalnya, berdasarkan sejumlah kasus penipuan dengan teknik rekayasa sosial di Indonesia, para korban seringkali belum memahami pentingnya keamanan sebagai pengguna teknologi digital.

26. Lihat Lampiran.

Rekomendasi Pencegahan Penipuan dengan Teknik Rekayasa Sosial: Pendidikan, Pelatihan, dan Peningkatan Kesadaran

Pendekatan yang bertujuan untuk meningkatkan resiliensi 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.

Peran aktif setiap pemangku kepentingan diperlukan untuk melawan penipuan dengan teknik rekayasa sosial

Pendekatan melalui kebijakan dan inisiatif di luar pendidikan formal juga diperlukan untuk menyasar peningkatan kompetensi keamanan seluruh masyarakat Indonesia yang telah atau berpotensi menggunakan layanan teknologi. Oleh karena target audiensnya yang luas, pendekatan ini harus melibatkan berbagai pemangku kepentingan terkait dengan metode yang berbeda-beda sesuai dengan kapasitas pemangku kepentingan tersebut. Berikut adalah upaya yang dapat dilakukan setiap pemangku kepentingan dalam melaksanakan pencegahan melalui kebijakan dan inisiatif:

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.[27] 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 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.

[27] Lebih lanjut mengenai kewajiban perusahaan fintech (dikenal sebagai Pelaku Usaha Jasa Keuangan (PUJK)) terkait keamanan pengguna fintech, lihat Peraturan Otoritas Jasa Keuangan Nasional nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan, pasal 14.

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

  Peningkatan kompetensi keamanan melalui paltform 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 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 menyasar 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

Industri teknologi membutuhkan dukungan serta kolaborasi dengan pemerintah dan regulator untuk dapat meningkatkan kompetensi keamanan pengguna teknologi. Dukungan yang dibutuhkan dimulai dari kebijakan yang mengedepankan peningkatan edukasi pengguna teknologi, hingga kerjasama lintas industri (misalnya industri perbankan, keuangan, telekomunikasi, teknologi informasi, dan lainnya) agar upaya kegiatan edukasi dapat menjangkau masyarakat secara luas.

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.

Dari segi upaya kegiatan, 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. Selebihnya, 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.[28]

[28] Lebih lanjut mengenai kolaborasi pemerintah dan regulator dengan industri teknologi, lihat World 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.

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/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 (diolah oleh penulis)

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 menyasar 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 Furnell,[29] serta Cone dkk.[30] Pendekatan seperti ini telah dicoba oleh DROG[31], 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.[32] 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.

[29] Lebih lanjut mengenai pendekatan melalui video game yang diusulkan oleh Newfound dan Furnell, lihat Newbould, 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 Jan 2020].

[30] Lebih lanjut mengenai pendekatan melalui video game yang diusulkan oleh Cone dkk., lihat Cone, 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.

[31] Lebih lanjut mengenai DROG, lihat DROG. (n.d.) A Good Way to Fight Bad News. [daring] Dapat diakses pada https://www.aboutbadnews.com/.

[32] Lebih lanjut mengenai Bad News Game, lihat Bad News Game. (n.d.) How Does Bad News Work?. [daring] Dapat diakses pada https://getbadnews.com/#intro.

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 menyasar 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.

Glosarium

Call Forwarding	Fitur dalam telefon yang menyambungkan panggilan kepada pihak lain
Fintech (Financial Technology)	Servis finansial berbasis teknologi untuk memberi kemudahan bagi pengguna
Literasi Digital	Pengetahuan dan kecakapan penggunaan media digital, alat-alat komunikasi, atau jaringan dalam memahami manfaat dan resiko di dalamnya.
OTP *(One-Time Password)*	Kata sandi yang yang hanya bisa digunakan sekali dalam sebuah transaksi
Penipuan dengan Teknik Rekayasa Sosial	Penipuan yang menggunakan kemampuan pelaku penipuan untuk membangun kepercayaan korban dan memanfaatkan kepercayaan (manipulasi psikologi) tersebut untuk melaksanakan serangan penipuannya

Lampiran

Kasus Penipuan dengan Teknik Rekayasa Sosial

Penipuan Rekayasa Sosial - **Bank Konvensional**

1. **Go Mobile CIMB Niaga tidak Aman**
   https://mediaindonesia.com/read/detail/70525-go-mobile-cimb-niaga-tidak-aman
2. **Penipuan Kartu Kredit Terungkap dari SMS Konfirmasi**
   https://megapolitan.kompas.com/read/2013/09/27/1634320/Penipuan.Kartu.Kredit.Terungkap.dari.SMS.Konfirmasi.
3. **Bos Tipu-tipu SMS Modus 'Mama Minta Pulsa' Dibekuk**
   https://news.detik.com/berita/3062973/bos-tipu-tipu-sms-modus-mama-minta-pulsa-dibekuk
4. **Waspada! Modus Mengganjal Kartu ATM, 2 Pembobol Gasak Rp40 Juta**
   https://news.okezone.com/read/2017/11/23/525/1819190/waspada-modus-mengganjal-kartu-atm-2-pembobol-gasak-rp40-juta
5. **Warga Bekasi Tertipu Call Center ATM Palsu, Rp 68 Juta Ludes**
   https://news.detik.com/berita/d-2917974/warga-bekasi-tertipu-call-center-atm-palsu--68-juta-ludes
6. **Polisi Bongkat Penipu Berkedok Call Center Palsu di ATM**
   https://nasional.republika.co.id/berita/nasional/jabodetabek-nasional/18/11/06/phs29e430-polisi-bongkat-penipu-berkedok-call-center-palsu-di-atm
7. **Polisi Ungkap Tersangka Baru Pembobol Bank DBS**
   https://www.jpnn.com/news/polisi-ungkap-tersangka-baru-pembobol-bank-dbs?page=2
8. **BRI Tutup Layanan Debit dan Kartu Kredit Ayopop**
   https://www.jpnn.com/news/bri-tutup-layanan-debit-dan-kartu-kredit-ayopop?page=2

Penipuan Rekayasa Sosial - **Jasa Asuransi**

1. **Pemalsuan Kartu BPJS Sudah Berlangsung Setahun**
   https://mediaindonesia.com/read/detail/58073-pemalsuan-kartu-bpjs-sudah-berlangsung-setahun

Penipuan Rekayasa Sosial - **Jasa Layanan Teknologi**

1. **Hati-Hati! Jangan Klik Pesan Teks Ini di WhatsApp**
   https://techno.okezone.com/read/2017/11/19/207/1816733/hati-hati-jangan-klik-pesan-teks-ini-di-whatsapp
2. **Korban Arisan Online "Mama Yona" Terus Berdatangan dari Luar Bekasi**
   https://megapolitan.okezone.com/read/2018/02/13/338/1858784/korban-arisan-online-mama-yona-terus-berdatangan-dari-luar-bekasi
3. **WNA Penipu Via Facebook Diringkus di Medan**
   https://regional.kompas.com/read/2013/06/10/04082443/WNA.Penipu.Via.Facebook.Diringkus.di.Medan.
4. **WNA Nigeria kirim 3.781 pesan penipuan Facebook**
   https://www.antaranews.com/berita/403216/wna-nigeria-kirim-3781-pesan-penipuan-facebook

Penipuan Rekayasa Sosial - **e-Wallet**

1. **Kasus Pembobolan Akun Gojek Aura Kasih Mirip Mama Minta Pulsa**
   https://www.liputan6.com/tekno/read/4113679/kasus-pembobolan-akun-gojek-aura-kasih-mirip-mama-minta-pulsa
2. **Maia Estianty Kena Penipuan Ojol Pakai Modus dengan Kode **21* Ini Penjelasannya: Fitur Call Forward**
   https://www.tribunnews.com/lifestyle/2020/01/01/maia-estianty-kena-penipuan-ojol-pakai-modus-dengan-kode-21-ini-penjelasannya-fitur-call-forward.

Penipuan Rekayasa Sosial - **Industri Telekomunikasi**

1. **17 Orang Sindikat Penipuan Undian Mengaku-ngaku Telkomsel Dibekuk Polisi**
   https://news.detik.com/berita/2347002/17-orang-sindikat-penipuan-undian-mengaku-ngaku-telkomsel-dibekuk-polisi
2. **Begini Aneka Rupa SMS Esek-esek yang Mengarahkan ke 0809xxxxx**
   https://news.detik.com/berita/d-2914860/begini-aneka-rupa-sms-esek-esek-yang-mengarahkan-ke-0809xxxxx
3. **Telkomsel Imbau Pelanggan Waspada Penipuan Mengatasnamakan Telkomsel**
   https://palembang.tribunnews.com/2018/01/22/telkomsel-imbau-pelanggan-waspada-penipuan-mengatasnamakan-telkomsel.
4. **Telkomsel: Jangan Pernah Beri Kode dan Password, Awas Penipuan**
   https://www.viva.co.id/digital/digilife/1091655-telkomsel-jangan-pernah-beri-kode-dan-password-awas-penipuan
5. **Mengenal Penipuan SIM Swap yang Bikin Ilham Bintang 'Boncos'**
   https://www.cnnindonesia.com/teknologi/20200120122555-185-466929/mengenal-penipuan-sim-swap-yang-bikin-ilham-bintang-boncos
6. **Penipuan Modus Baru WhatsApp, Kominfo Imbau Waspada dengan Nomor Baru**
   https://www.jawapos.com/oto-dan-tekno/teknologi/04/12/2018/penipuan-modus-baru-whatsapp-kominfo-imbau-waspada-dengan-nomor-baru/

Penipuan Rekayasa Sosial - **e-Commerce**

1. **Pengakuan Korban Penipuan Berkedok Traveloka di Pontianak, Ungkap Modus Pelaku**
   https://pontianak.tribunnews.com/2019/07/17/pengakuan-korban-penipuan-berkedok-traveloka-di-pontianak-ungkap-modus-pelaku.
2. **Waspada! Marak SMS Penipuan Sejak THR Cair**
   https://finance.detik.com/moneter/d-4066355/waspada-marak-sms-penipuan-sejak-thr-cair
3. **Warga Aceh Timur Tertipu Undian Online Berhadiah, Rp 17 Juta Raib**
   https://aceh.tribunnews.com/2019/06/08/warga-aceh-timur-tertipu-undian-online-berhadiah-rp-17-juta-raib.
4. **Tipu-tipu Jualan Online! Tokopedia Tutup Penjual 'Gambar Hard Disk'**
   https://news.detik.com/berita/d-4301481/tipu-tipu-jualan-online-tokopedia-tutup-penjual-gambar-hard-disk
5. **Sindikat Penipuan via SMS Kelompok Sidrap Mengaku Agen Tiket Traveloka**
   https://news.detik.com/berita/d-2787793/sindikat-penipuan-via-sms-kelompok-sidrap-mengaku-agen-tiket-traveloka

Center for Digital Society

Faculty of Social and Political Sciences
Universitas Gadjah Mada
Room BC 201-203, BC Building 2nd Floor,
Jalan Socio Yustisia 1
Bulaksumur, Yogyakarta, 55281, Indonesia

Phone : (0274) 563362, Ext. 116
Email : cfds.fisipol@ugm.ac.id
Website : cfds.fisipol.ugm.ac.id

facebook.com/cfdsugm
cfds.fisipol.ugm.ac.i d
cfds_ugm
@cfds_ugm
@cfds_ugm
CfDS UGM