DOI: 10.12962/j26139960.v6i2.92 | Naskah Masuk 27-07-2021; | Naskah Diulas 24-08-2021; | Naskah Diterima 12-02-2022

NASKAH ORISINAL

Sosialisasi Bahaya dan Upaya Pencegahan *Social Engineering* untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi

Eko Wahyu Tyas Darmaningrat[1,*] | Achmad Holil Noor Ali[1] | Anisah Herdiyanti[1] | Apol Pribadi Subriadi[1] | Feby Artwodini Muqtadiroh[1] | Hanim Maria Astuti[1] | Tony Dwi Susanto[1]

[1]Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

Korespondensi

*Eko Wahyu Tyas Darmaningrat, Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia. Alamat e-mail: tyas@is.its.ac.id

Alamat

Laboratorium Manajemen Sistem Informasi (MSI), Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

Abstrak

Pada tahun 2018, pengguna media sosial di Indonesia mencapai 49% dari total penduduk Indonesia yaitu 130 juta dari total 265,4 juta populasi. Perilaku *upload* foto, video, atau tulisan yang berisikan informasi pribadi dapat menyebabkan pengguna berada dalam posisi yang berbahaya dan berpotensi hilangnya privasi pengguna. Banyak dari kasus kriminal dilakukan dengan tujuan untuk mendapatkan keuntungan. Pelaku mengambil foto dan informasi nomor seluler korban melalui sosial media dan mengedit foto korban menjadi foto vulgar untuk mengancam dan memeras korban. Kasus penyalahgunaan informasi disebabkan oleh kurangnya kesadaran untuk menjaga privasi informasi di media sosial. *Social engineering* merupakan salah satu teknik yang perlu diwaspadai dalam menjaga keamanan informasi. *Social engineering* berfokus pada bagian terlemah pada sistem jaringan komputer, yaitu manusia. Teknik ini berusaha mengambil informasi pribadi dengan melakukan manipulasi psikologis melalui mekanisme interaksi sosial. Selain itu, dalam pelaksanaan *social engineering*, pelaku meminta langsung apa yang diinginkan. Berdasarkan permasalahan tersebut, tim pengabdi melakukan sosialisasi mengenai berbagai teknik *social engineering*, dampak yang ditimbulkan, serta upaya pencegahannya kepada masyarakat. Adanya kebijakan WFH di era pandemi COVID-19 saat ini mengakibatkan penggunaan *gadget* dan media sosial semakin massif. Sebagian besar peserta berpendapat bahwa materi yang disampaikan menarik. Hal ini membuat peserta sangat antusias dan menyampaikan cukup banyak pertanyaan. Setelah mengikuti sosialisasi, peserta menjadi lebih berhati-hati jika hendak membagikan foto atau informasi yang mungkin mengandung informasi pribadi di media sosial.

Kata Kunci:

Social Engineering, Keamanan Informasi, Kelompok Masyarakat, Kualitas Air.

1 | PENDAHULUAN

Pada tahun 2019, total jumlah pengguna telepon seluler di Indonesia mencapai 355,5 juta, jauh lebih banyak dari total jumlah penduduk Indonesia, 133%. Dari jumlah itu 97% nya adalah pengguna kartu Pra Bayar sementara hanya 3% saja yang menggunakan kartu Paska Bayar. Sedangkan penetrasi akses ke 3G dan 4G mencapai 84%[1]. Selain itu, total pengguna aktif media sosial di Indonesia mencapai 150 juta pengguna. Hal ini berarti mayoritas penggunaan internet bersosialisasi melalui media sosial. Jumlah pengguna media sosial ini mencapai 56% dari jumlah total penduduk Indonesia, dengan pengguna berbasis mobile mencapai 130 juta. Hal ini memicu semua *platform* media sosial akhirnya fokus untuk optimalisasi aplikasinya di perangkat mobile[1].

Saat ini banyak ibu rumah tangga yang berbisnis dari rumah dan menggunakan media sosial sebagai alat promosi. Media sosial merupakan alat promosi bisnis yang efektif karena dapat diakses oleh siapa saja, sehingga jaringan promosi bisa lebih luas. Media sosial menjadi bagian yang sangat diperlukan oleh pemasaran bagi banyak perusahaan dan merupakan salah cara terbaik untuk dapat menjangkau luasnya pasar ataupun pelanggan. Media sosial seperti facebook, twitter, instagram, dan youtube memiliki sejumlah manfaat sendiri bagi para pelaku usaha dibandingkan dengan menggunakan media konvensional sebagai media promosi[2].

Anak-anak dan remaja saat ini merupakan golongan masyarakat yang hidup di era *digital* (*digital native*). Sementara itu, generasi orang tua dari mereka saat ini masih cenderung menjadi penduduk pendatang digital (*digital immigrant*). Akibatnya, kesadaran akan potensi negatif yang mengancam anak-anak dan remaja tidak disadari dan diseriusi oleh kalangan dewasa. Anak dan remaja dapat digambarkan sebagai digital native, merupakan kalangan serupa penduduk asli di dunia digital saat ini. Mereka lahir dan tumbuh di era *digital* yang menjadikan mereka memiliki cara berpikir, berbicara, dan bertindak berbeda dengan generasi sebelumnya yang diibaratkan sebagai digital immigrant[3].

Dalam menggunakan media sosial, remaja memiliki sifat yang cukup terbuka karena adanya keinginan untuk tetap eksis dengan melakukan upload kegiatan yang sedang mereka lakukan dalam bentuk foto, video, maupun tulisan. Perilaku *upload* foto, video, atau tulisan yang seringkali berisikan informasi pribadi mereka tersebut dapat menyebabkan pengguna berada dalam posisi yang berbahaya dan berpotensi hilangnya privasi pengguna. Beberapa kasus kriminal seputar penyalahgunaan informasi kerap kali terjadi di Indonesia. Banyak dari kasus tersebut dilakukan dengan tujuan untuk mendapatkan keuntungan. Pelaku mengambil foto dan informasi nomor seluler korban melalui sosial media dan mengedit foto korban menjadi foto vulgar. Foto tersebut digunakan sebagai umpan untuk mengancam korban dan memeras korban. Kasus mengenai penyalahgunaan informasi tersebut disebabkan oleh kurangnya kesadaran akan pentingnya menjaga privasi informasi di media sosial. Orang tua, khususnya ibu, mempunya peranan yang sangat dalam mengarahkan penggunaan teknologi secara aman bagi keluarga dan masyarakat di sekitarnya.

Social engineering merupakan salah satu teknik yang perlu diwaspadai dalam menjaga keamanan informasi. *Social engineering* berfokus pada bagian terlemah pada sistem jaringan komputer, yaitu manusia. *Social engineering* merupakan salah satu teknik *hacking* yang paling mudah di lakukan karena dilakukan dengan mengeksploitasi kelemahan manusia seperti rasa takut, rasa percaya, dan rasa ingin menolong. Pada dasarnya teknik *social engineering* terbagi menjadi dua jenis, yaitu berbasis interaksi sosial dan berbasis interaksi komputer[4]. Menurut eksperimen yang dilakukan oleh Bullée et al.[5], peningkatan kesadaran tentang bahaya, karakteristik, dan penanggulangan yang terkait dengan *social engineering* terbukti memiliki efek positif yang signifikan dalam menetralisir penyerangan. Melalui kegiatan pengabdian ini diharapkan dapat meningkatkan kesadaran dan kepedulian masyarakat terhadap keamanan informasi.

Mengacu kepada latar belakang permasalahan yang telah dijelaskan tersebut, beberapa permasalahan mitra yang kami identifikasi antara lain mencakup:

1. Pengguna Internet dan media sosial terbanyak adalah pada rentang usia remaja (18–34 tahun). Orang tua, khususnya ibu, mempunya peranan yang sangat penting dalam mengarahkan penggunaan teknologi secara aman bagi keluarga dan masyarakat di sekitarnya.
2. *Social engineering* merupakan salah satu teknik hacking yang paling mudah di lakukan karena dilakukan dengan mengeksploitasi kelemahan manusia seperti rasa takut, rasa percaya, dan rasa ingin menolong.

Peningkatan kesadaran tentang bahaya, karakteristik, dan penanggulangan yang terkait dengan *social engineering* terbukti memiliki efek positif yang signifikan dalam menetralisir penyerangan.

Untuk memberikan solusi bagi permasalahan yang dihadapi oleh mitra, kegiatan pengabdian masyarakat ini memberikan sosialisasi mengenai bahaya *social engineering*, berbagai metode dan teknik *social engineering*, serta upaya pencegahan yang dapat dilakukan bagi kelompok ibu tim penggerak PKK (Pembinaan Kesejahteraan Keluarga) di Kelurahan Mojo, Kecamatan Gubeng, Kota Surabaya. Kruger dan Kearney mengembangkan model prototipe untuk mengukur kesadaran keamanan informasi di perusahaan pertambangan emas internasional berdasarkan *knowlodge* (pengetahuan), *attitude* (sikap), dan *Behavior* (perilaku)[6]. Model *Knowledge-Attitude-Behavior* (KAB) menjelaskan bahwa perilaku berubah secara bertahap. Ketika pengetahuan terakumulasi, kemudian perubahan sikap dimulai, selanjutnya perubahan sikap menumpuk dan menghasilkan perubahan perilaku.

Pengabdian masyarakat ini fokus pada aspek peningkatan pengetahuan (*knowledge*). Pelaksanaan kegiatan ini diharapkan dapat meningkatkan kesadaran masyarakat tentang keamanan informasi sehingga dapat merubah sikap (*attitude*) mereka dalam membagikan informasi pribadi di media sosial dan internet serta selanjutnya hal ini dapat menjadi perilaku keseharian mereka (*behavior*). Bentuk pelaksanaan dari kegiatan pengabdian ini adalah berupa sosialisai dan workshop meningkatkan kesadaran keamanan informasi kelompok ibu PKK dengan cara:

1. Memberikan sosialisasi tentang teknik *social engineering* dan bahayanya.
2. Memberikan contoh kasus-kasus pelanggaran yang pernah terjadi sehingga mereka mempunyai gambaran riil tentang praktik *social engineering*.
3. Melakukan praktik pencegahan *social engineering* sederhana melalui telepon selular.

2 | TINJAUAN PUSTAKA

2.1 | *Social Engineering*

Menurut SANS Institute, *social engineering* adalah serangan psikologis di mana penyerang menipu korban untuk melakukan sesuatu yang seharusnya tidak dilakukan[7]. Konsep *social engineering* bukanlah hal baru; namun yang membuat teknologi saat ini jauh lebih efektif bagi para penyerang dunia maya adalah korban tidak dapat melihatnya secara fisik; pelaku dapat dengan mudah berpura-pura menjadi apa pun atau siapa pun yang mereka inginkan dan menargetkan jutaan orang di seluruh dunia. Selain itu, serangan *social engineering* dapat melewati banyak teknologi keamanan. Kesalahpahaman umum yang dimiliki kebanyakan orang tentang penyerang dunia maya adalah bahwa pelaku menggunakan alat dan teknik yang sangat canggih untuk meretas ke komputer atau akun korban. Padahal, penyerang dunia maya telah belajar bahwa seringkali cara termudah untuk mencuri informasi pribadi, meretas akun, atau menginfeksi sistem korban adalah dengan menipu korban agar melakukan kesalahan.

Serangan *social engineering* datang dalam berbagai bentuk dan dapat dilakukan di mana saja dengan melibatkan interaksi manusia. Berikut ini adalah lima bentuk paling umum dari serangan *social engineering* secara digital[8].

2.1.1 | *Baiting*

Seperti namanya, serangan ini menggunakan janji palsu untuk menyinggung keserakahan atau keingintahuan korban. Mereka memikat pengguna ke dalam perangkap untuk mencuri informasi pribadi mereka atau membuat sistem mereka terinfeksi *malware*. Contoh umpan menggunakan media fisik untuk memyebarkan *malware* misalnya penyerang meninggalkan umpan (biasanya *flash drive* yang terinfeksi *malware*) di area yang mencolok di mana calon korban yakin melihatnya (misal: kamar mandi, *lift*, tempat parkir perusahaan yang ditargetkan). Umpan tersebut memiliki tampilan otentik, seperti label yang menyajikan informasi sebagai daftar gaji perusahaan. Para korban mengambil umpan karena penasaran dan memasukkannya ke komputer kantor atau rumah, yang menghasilkan pemasangan *malware* otomatis pada sistem. Penipuan ini tidak harus dilakukan di dunia fisik. Bentuk umpan *online* terdiri dari iklan menarik yang mengarah ke situs jahat atau yang mendorong pengguna untuk mengunduh aplikasi yang terinfeksi *malware*.

2.1.2 | *Pretexting*

Dalam teknik ini seorang penyerang mendapatkan informasi melalui serangkaian kebohongan yang dibuat dengan cerdik. Penipuan ini sering diprakarsai oleh pelaku yang berpura-pura membutuhkan informasi sensitif dari seorang korban untuk melakukan tugas penting. Pelaku biasanya mulai membangun kepercayaan dengan korban dengan cara meniru rekan kerja, polisi, pejabat bank dan pajak, atau orang lain yang memiliki wewenang untuk mengetahui. *Pretexter* mengajukan pertanyaan yang seolah-olah diperlukan untuk mengkonfirmasi identitas korban, yang melaluinya mereka mengumpulkan data pribadi yang penting. Berbagai jenis informasi penting dapat dikumpulkan menggunakan teknik ini, seperti nomor jaminan sosial, alamat pribadi dan nomor telepon, catatan telepon, tanggal liburan staf, catatan bank, dan bahkan informasi keamanan yang berkaitan dengan pabrik fisik.

2.1.3 | *Phising*

Sebagai salah satu jenis serangan *social engineering* yang paling populer, penipuan phising adalah kampanye email dan pesan teks yang ditujukan untuk menciptakan rasa urgensi, keingintahuan atau ketakutan pada korban. Hal ini kemudian mendorong mereka untuk mengungkapkan informasi sensitif, mengklik tautan ke situs web jahat, atau membuka lampiran yang mengandung *malware*. Contohnya adalah *email* yang dikirimkan kepada pengguna layanan *online* yang memberi tahu mereka tentang pelanggaran kebijakan yang membutuhkan tindakan segera dari pihak mereka, seperti perubahan kata sandi yang diperlukan. Ini termasuk tautan ke situs web tidak sah — penampilannya hampir identik dengan versi yang sah — mendorong pengguna tidak curiga untuk memasukkan kredensial dan kata sandi baru mereka saat ini. Setelah pengisian formulir kemudian informasi tersebut dikirim ke penyerang. Karena pesan yang identik atau hampir identik dikirim ke semua pengguna dalam kampanye phishing, mendeteksi dan memblokirnya jauh lebih mudah bagi *server email* yang memiliki akses ke *platform* berbagi ancaman.

2.1.4 | *Tailgating*

Serangan *tailgating*, juga dikenal sebagai *piggybacking*, di mana penyerang berusaha mencari celah untuk masuk ke area terbatas yang tidak memiliki otentikasi yang tepat. Penyerang hanya bisa berjalan di belakang seseorang yang berwenang untuk mengakses area tersebut. Dalam tipikal skenario serangan, seseorang menyamar sebagai sopir pengiriman atau pengasuh yang dikemas dengan paket dan menunggu ketika seorang karyawan membuka pintu mereka. Penyerang meminta karyawan menahan pintu, melewati langkah-langkah keamanan yang berlaku (mis. Kontrol akses elektronik).

2.1.5 | *Whaling Attack*

Whaling Attack adalah evolusi lain dari serangan phishing yang menggunakan teknik *social engineering* yang canggih untuk mencuri informasi rahasia, data pribadi, akses kredensial ke layanan / sumber daya terbatas, dan khususnya informasi dengan nilai yang relevan dari perspektif ekonomi dan komersial. Perbedaan kategori *phishing* ini dari yang lain adalah pilihan targetnya, yaitu eksekutif relevan dari bisnis swasta dan lembaga pemerintah. Kata *Whaling Attack* digunakan untuk menunjukkan bahwa targetnya adalah ikan besar untuk ditangkap. *Whaling Attack* mengadopsi metode yang sama dari serangan *spear phishing*, tetapi *email* penipuan dirancang untuk menyamar sebagai *email* bisnis penting yang dikirim dari otoritas yang sah, biasanya dari eksekutif terkait organisasi penting. Isi pesan yang dikirim dirancang untuk manajemen tingkat atas dan melaporkan semacam kekhawatiran palsu di seluruh perusahaan atau informasi rahasia yang tinggi.

2.2 | Keamanan Informasi

The Committee on National Security Systems (CNSS) mendefinisikan keamanan informasi sebagai perlindungan terhadap informasi dan elemen kritisnya termasuk sistem dan perangkat keras yang digunakan, penyimpanan, dan proses pengiriman informasi[9]. Keamanan informasi juga dapat diartikan sebagai upaya untuk melindungi informasi dan sistem informasi dari akses oleh pihak yang tidak berwewenang, dalam hal penggunaan, penyikapan, gangguan, modifikasi, maupun perusakan yang tidak sah untuk menjaga aspek keamanan informasi, seperti integritas, kerahasiaan, dan ketersediaan informasi[10].

2.3 | Kesadaran Keamanan Informasi

Pengertian kesadaran keamanan informasi dijelaskan dalam *Information Security Forum* (ISF), yaitu "Kesadaran terhadap keamanan teknologi informasi adalah tingkat atau jangkauan pemahaman dari setiap anggota dalam organisasi mengenai pentingnya keamanan teknologi informasi, level keamanan teknologi informasi yang sesuai dengan organisasi, dan tanggung jawab terhadap keamanan informasi secara individu"[11]. Shaw at al mengartikan kesadaran keamanan informasi sebagai tingkat pemahaman pengguna tentang pentingnya keamanan informasi dan memahami tanggung jawab mereka, serta mengetahui tindakan untuk mengkontrol keamanan informasi yang cukup untuk melindungi data dan jaringan dalam organisasi[12]. Tujuan dari meningkatkan kesadaran akan keamanan informasi adalah membuat perubahan positif pada perilaku orang-orang yang terlibat dalam sebuah organisasi, sehingga pengetahuan mengenai keamanan informasi dalam hal ini merupakan hal penting guna menyadarkan orang-orang, baik secara individual maupun dalam organisasi akan risiko yang mereka hadapi dan merangsang mereka untuk mencegah risiko tersebut agar tidak terjadi[13].

3 | METODE PELAKSANAAN KEGIATAN

Metode pelaksanaan kegiatan pada program pengabdian masyarakat ini berupa:

3.1 | Sosialisasi (webinar)

Kegiatan sosialisasi atau webinar tentang teknik *social engineering* dan bahayanya dalam bentuk presentasi dan tanya jawab diharapkan dapat memberikan pengetahuan (*knowledge*) kepada mitra tentang berbagai metode social engineering. Dikarenakan masih belum memungkinkan untuk mengumpulkan massa dalam jumlah besar, maka kegiatan sosialisasi kami lakukan secara daring dengan menggunakan *Zoom meeting* dan Youtube *live stream*. Rencana awal kegiatan ini hanya diperuntukkan bagi kelompok ibu-ibu PKK di wilayah Kelurahan Mojo, Kecamatan Gubeng Surabaya. Namun karena kegiatan dilakukan secara daring, maka kami membuka kesempatan bagi lebih banyak kelompok masyarakat untuk bergabung dalam kegiatan ini.

3.2 | Simulasi

Simulasi pelaksanaan praktik *social engineering* dengan memberikan contoh kasus-kasus pelanggaran yang pernah terjadi. Hal ini diharapkan dapat gambaran riil tentang praktik *social engineering* kepada mitra, sehingga mereka lebih aware jika nantinya berada dalam kondisi tersebut (menjadi sasaran target pelaksanaan *social engineering*).

3.3 | Praktik

Praktik pencegahan *social engineering* sederhana melalui pengaturan *privacy* pada berbagai media sosial yang digunakan mitra dan juga pengaturan *privacy* pada telepon selular.

3.4 | Penyebaran Poster dan Video

Penyebaran poster dan video tentang teknik-teknik *social engineering* dan upaya pencegahannya. Poster versi cetak akan kami tempelkan di balai RT dan balai RW di lingkungan Kelurahan Mojo yang menjadi mitra kegiatan ini. Selain itu poster dan video juga akan disebarkan melalui grup WhatsApp dan berbagai media sosial sehingga informasi tersebut dapat menjangkau masyarakat luas.

4 | HASIL PELAKSANAAN KEGIATAN

Berikut adalah hasil dari pelaksanaan kegiatan pengabdian kepada masyarakat yang telah kami lakukan.

4.1 | Sosialisasi (Webinar)

Kegiatan sosialisasi (webinar) tentang teknik social engineering dan bahayanya ini dihadiri oleh 55 peserta di *Zoom meeting* dan diikuti oleh 230 *viewers* di Youtube. Kegiatan dilaksanakan dalam bentuk presentasi dan tanya jawab. Gambar 2 berikut

merupakan hasil dokumentasi kegiatan webinar melalui *Zoom meeting*, sedangkan Gambar 3 merupakan dokumentasi kegiatan yang disiarkan secara live di channel Youtube Depatemen Sistem Informasi, Institut Teknologi Sepuluh Nopember.

Gambar 1 Dokumentasi pelaksanaan kegiatan sosialisasi (webinar) di zoom.

Gambar 2 Dokumentasi pelaksanaan kegiatan sosialisasi (webinar) di youtube.

Peserta kegiatan ini terdiri dari berbagai kalangan, mulai dari ibu rumah tangga, guru, pelajar, dan mahasiswa. Peserta cukup antusias mengikuti kegiatan ini dan aktif dalam diskusi dan tanya jawab.

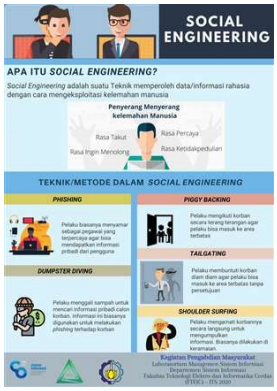
4.2 | Simulasi dan Praktik

Dalam acara webinar, kami memberikan simulasi mengenai praktik pencurian data dan informasi pribadi dari contoh kasus korban social engineering sebagaimana ilustrasi pada Gambar 3. Hal ini dapat gambaran riil tentang praktik *social engineering* kepada mitra, sehingga mereka lebih waspada jika nantinya berada dalam kondisi tersebut (menjadi sasaran target pelaksanaan *social engineering*). Dalam diskusi, peserta cukup aktif bertanya tentang kondisi riil yang ada di Indonesia dan kejadian yang pernah mereka alami serta bagaimana solusi yang sebaiknya dilakukan. Kasus yang dibahas sangat bervariasi mulai dari kasus terkait undang-undang perlindungan informasi pribadi, kasus investasi, penipuan, dan lain-lain.

Gambar 3 Simulasi pencurian informasi pribadi dalam kegiatan sosialisasi (Webinar) di youtube.

4.3 | Penyebaran Poster dan Video

Poster versi cetak kami tempelkan di balai RT dan balai RW di lingkungan Kelurahan Mojo yang menjadi mitra kegiatan ini. Selain itu poster dan video juga disebarkan melalui grup WhatsApp dan berbagai media sosial (Youtube, Facebook, Instagram, dan Twitter) sehingga informasi tersebut dapat menjangkau masyarakat luas. Poster pada Gambar 4 menjelaskan tentang definisi *social engineering* dan beberapa teknik yang umum dipakai oleh penyerang dalam aksinya, antara lain *phishing*, *dumpster diving*, *piggy backing*, *tailgating*, dan *shoulder surfing*.



Gambar 4 Poster tentang definisi dan teknik dalam *social engineering*.

Selanjutnya, poster pada Gambar 5 menjelaskan tentang proses-proses yang ada dalam *social engineering*, yaitu mulai dari tahapan pengumpulan informasi, menjalin hubungan dengan calon korban, eksekusi, dan eksploitasi kelemahan korban.

Untuk meminimalisir korban *social engineering* dan meningkatkan kesadaran akan pentingnya perlindungan informasi pribadi, kami juga menyebarkan poster yang berisi bagaimana upaya pencegahan *social engineering* yang dapat kita lakukan, seperti terlihat pada Gambar 6. Kami menyebarkan poster ke mitra melalui Grup WhatsApp yang diikuti peserta serta melalui berbagai media sosial, antara lain Facebook, Instagram, dan Twitter.

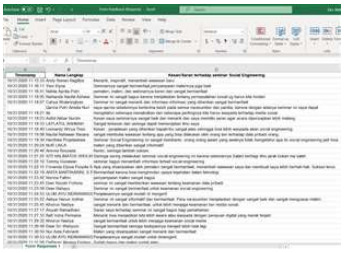
Selain poster, kami juga menyajikan informasi terkait *social engineering* dan upaya pencegahannya di channel Youtube Departemen Sistem Informasi ITS seperti ditunjukkan pada Gambar 7 dan Gambar 8.

Gambar 5 Poster tentang proses dalam *social engineering*.

Gambar 6 Poster tentang upaya pencegahan *social engineering*.

Gambar 7 Video pengenalan *social engineering* di youtube.

Gambar 8 Video upaya pencegahan *social engineering* di youtube.



Gambar 9 Form *feedback* peserta kegiatan pengabdian.

4.4 | *Feedback* dari Mitra Kegiatan

Adanya kebijakan *work-from-home* (WFH) dan *study-from-home* (SFH) di era pandemi COVID-19 saat ini mengakibatkan penggunaan *gadget* dan media sosial semakin massif. Hal ini membuat peserta kegiatan webinar mengenai bahaya dan upaya pencegahan *social engineering* sangat antusias dan menyampaikan cukup banyak pertanyaan dalam sesi tanya jawab. Berikut merupakan feedback dari beberapa peserta yang telah mengikuti kegiatan. Sebagian besar berpendapat bahwa materinya menarik

dan sangat sesuai dengan kondisi saat ini. Semua peserta juga bersedia untuk dikontak kembali apabila ada kegiatan serupa atau kegiatan pengabdian masyarakat lainnya di tahun-tahun mendatang.

Setelah mengikuti sosialisasi, peserta menjadi berpikir ulang dan lebih berhati-hati jika hendak membagikan foto atau informasi yang mungkin mengandung informasi pribadi di media sosial.

5 | KESIMPULAN

Kondisi pandemi yang terjadi mengharuskan kami merubah strategi pelaksanaan kegiatan, namun tidak mengurangi besarnya manfaat dan dampak yang diperoleh oleh masyarakat dari pelaksanaan kegiatan ini. Kegiatan berbasis daring mempunyai sisi positif, salah satunya adalah dapat diikuti oleh lebih banyak masyarakat dan bisa menjangkau lingkungan yang lebih luas. Transformasi digital yang terjadi akibat pandemi COVID-19 membuat kegiatan ini semakin relevan dengan kebutuhan masyarakat. Penggunaan teknologi harus didukung dengan kesadaran akan pentingnya menjaga keamanan informasi, sehingga dapat menghindarkan masyarakat dari berbagai dampak negatif yang mungkin ditimbulkan oleh oknum tidak bertanggung jawab dalam penggunaan teknologi tersebut. Berdasarkan *feedback* yang diberikan oleh peserta kegiatan, sebagian besar berpendapat bahwa materi yang disampaikan dalam kegiatan ini menarik dan sangat sesuai dengan kondisi saat ini. Semua peserta juga bersedia untuk dikontak kembali apabila ada kegiatan serupa atau kegiatan pengabdian masyarakat lainnya di tahun-tahun mendatang. Setelah mengikuti sosialisasi, peserta menjadi berpikir ulang dan lebih berhati-hati jika hendak membagikan foto atau informasi yang mungkin mengandung informasi pribadi di media sosial.

6 | UCAPAN TERIMA KASIH

Pengabdian masyarakat ini dibiayai oleh Direktorat Riset dan Pengabdian Kepada Masyarakat, Institut Teknologi Sepuluh Nopember, Surabaya melalui skema Pengabdian Masyarakat Dana Departemen sesuai dengan Surat Perjanjian Pelaksanaan Penelitian No: 1770/PKS/ITS/2020.

Referensi

1. Sindo. Indonesia Digital 2019, Januari 2019. https://websindocom/, Accessed 8 Maret 2020 2019;.
2. Prasetyo H. Media Sosial Sebagai Media Promosi Masa Kini?, Juli 2015. https://wwwkompasianacom/, Accessed 8 Maret 2020 2015;.
3. Firdaus D. Peran Orang Tua dalam Mengawasi Media Sosial, 30 Maret 2017. https://wwwnuorid/post/, Accessed 8 Maret 2020 2015;.
4. Peltier TR. Social engineering: Concepts and solutions. Information Security Journal 2006;15(5):13.
5. Bullée JWH, Montoya L, Pieters W, Junger M, Hartel PH. The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of experimental criminology 2015;11(1):97–115.
6. Kruger HA, Kearney WD. A prototype for assessing information security awareness. Computers & security 2006;25(4):289–296.
7. Institute S. SANS Security Awareness, Januari 2017. https://wwwsansorg/security-awareness-training/, Accessed 8 Maret 2020 2020;.
8. Imperva. Social Engineering Attack. https://wwwimpervacom/, Accessed 8 Maret 2020 2020;.
9. McConnell J. National Training Standard for Information Systems Security (INFOSEC) professionals. National Security Agency/Central Security Service Fort George G Meade Md; 1994.
10. Government U. Public Law 107–347 107th Congress Congress, Electron Gov. https://wwwsansorg/security-awareness-training/, Accessed 8 Maret 2020 2003;(2889–1970).

11. ISF. Effective Security Awareness. Information Security Forum (ISF), Accessed 8 Maret 2020 2002;.

12. Wilson M, Hash J, et al. Building an information technology security awareness and training program. NIST Special publication 2003;800(50):1–39.

13. Veseli. Measuring the effectiveness of information security awareness training 2007;.

Cara mengutip artikel ini: Tyas Darmaningrat, E. W., Noor Ali, A. H., Herdiyanti, A., Subriadi, A. P., Muqtadiroh, F. A., Astuti, H. M., Susanto, T. D., (2022), Sosialisasi Bahaya dan Upaya Pencegahan *Social Engineering* untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi, *Jurnal Sewagati*, *6(2):159–168*.