*Prosiding PKM-CSR, Vol. 4 (2021)*
*e-ISSN: 2655-3570*

# PENINGKATAN LITERASI DIGITAL MASYARAKAT TERHADAP *SOCIAL ENGINEERING* DALAM MASA PANDEMI COVID-19

**Theresia Herlina Rochadiani[1], Handri Santoso[2], Dennis Anthony Plaudo[3], Richard Setiawan[4], Vincensius Gilven Fiones[5]**
[1,2,3,4,5]Prodi Informatika Universitas Pradita

theresia.herlina@pradita.ac.id , handri.santoso@pradita.ac.id , dennis.anthony@student.pradita.ac.id, richard.setiawan@student.pradita.ac.id, vincensius.gilven@student.pradita.ac.id

**Abstrak**

Seluruh dunia, tak terkecuali Indonesia mengalami pandemi Covid-19 dari tahun 2020 sampai saat ini. Dengan adanya pandemi Covid-19 menyebabkan perubahan pola hidup masyarakat yang cenderung semakin banyak melakukan pekerjaan, kegiatan, dan transaksi secara daring daripada luring. Hal ini memicu semakin banyaknya kejahatan siber. Kejahatan siber di Indonesia masuk sebagai peringkat ke-2 di dunia. Dalam sistem jaringan komputer, manusia adalah komponen yang terlemah sehingga para penjahat siber memafaatkan hal ini dengan menggunakan *social engineering*, yaitu manipulasi psikologis korban, dalam melakukan kejahatan siber. Rendahnya literasi digital masyarakat akan keamanan siber membuat banyak masyarakat menjadi korban. Oleh karena itu, kegiatan PkM ini bertujuan untuk meningkatkan literasi digital masyarakat, khususnya akan *social engineering*, sehingga dapat menekan jumlah kejahatan siber. Metode pelaksanaan PkM ini meliputi tahapan : studi literatur terkait *social engineering*, membuat video edukasi contoh-contoh *social engineering* beserta mitigasinya, membuat kuesioner, dan video edukasi beserta kuesioner tersebut kemudian didiseminasikan secara daring, setelah itu diikuti dengan analisis hasil kuesioner dan penarikan kesimpulan untuk mengetahui apakah ada peningkatan literasi digital khususnya mengenai *social engineering* ini. Melalui survey yang dilaksanakan sebelum dan sesudah edukasi dapat dilihat adanya peningkatan literasi digital masyarakat akan *social engineering*, yaitu terjadi peningkatan dengan rata-rata persentase peningkatan dari 3 video edukasi sekitar 63.29%.

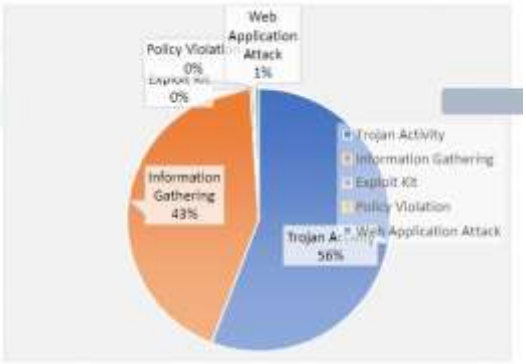
**Kata Kunci** : pandemi Covid-19, kejahatan siber, *social engineering*, literasi digital

## PENDAHULUAN

Di awal tahun 2020, dunia termasuk Indonesia mengalami pandemi Covid-19. Penularan melalui udara membuat diterapkannya pembatasan social di berbagai wilayah, bahkan diterapkan bekerja dari rumah atau dikenal dengan istilah *wfh* yang kepanjangannya adalah *work from home*. Oleh karena hal ini, pola hidup masyarakat berubah. Sekarang ini lebih banyak orang yang melakukan pekerjaan, kegiatan, dan transaksi secara daring daripada luring. Pandemi Covid-19 yang merubah

pola hidup masyarakat Indonesia menjadi lebih banyak menggunakan internet, mengakibatkan bertambahnya upaya serangan siber (Salsabila, 2020). Hal ini terlihat dari peningkatan jumlah kejahatan siber, seperti yang ditunjukkan pada gambar 1. Serangan siber yang terjadi di Indonesia pada tahun 2020 sebanyak 189.937.542, naik lima kali lipat dibandingkan pada tahun 2019 (Ikhsan, 2020).


Gambar 1. Jumlah Serangan Siber di Indonesia bulan Januari-Agustus 2019/2020 (Salsabila, 2020)




Gambar 2. Klasifikasi Serangan Siber Januari – April 2020 (Tobing, 2020)

Bentuk serangan siber beragam. Lima macam bentuk serangan terbanyak di Indonesia yang dapat dilihat dari gambar 2 adalah aktivitas trojan, pengumpulan informasi yang umumnya dilakukan dengan *social engineering*, kit eksploitasi, pelanggaran kebijakan, dan serangan aplikasi web. Dalam masa pandemi Covid ini melalui *social engineering*, para penjahat di dunia maya menawarkan bantuan jasa penyemprotan disinfektan di dalam rumah, sehingga penjahat mendapatkan akses fisik untuk masuk ke dalam rumah korban (Hadi et al, 2020).

Studi yang dilakukan Bakhshi (2017) dengan melakukan eksperimen serangan *social engineering* mendapatkan hasil dengan proporsi yang cukup tinggi, yaitu 45-60% orang gagal mengidentifikasi serangan dan menjadi korban dari serangan tersebut. Kurangnya kesadaran masyarakat menjadi penyebab utama keberhasilan serangan ini.

Sebagai salah satu aktor utama dalam pembentukan arsitektur keamanan dunia di era abad ke-21 (Arianto & Anggraini, 2019) Indonesia perlu mempersiapkan masyarakatnya untuk memiliki literasi keamanan siber. Oleh karena itu pemerintah melakukan upaya peningkatan literasi keamanan siber ini. Kominfo bekerja sama dengan BSSB, Bank Indonesia, dan Otoritas Jasa Keuangan melakukan upaya peningkatan kesadaran dan kapasitas masyarakat terkait keamanan seiber melalui webinar dan iklan layanan masyarakat serta pendampingan kepada perusahaan di semua sektor (Wicaksana et al., 2020). Tujuan utama dari program kesadaran dan pelatihan keamanan informasi adalah supaya para pekerja dapat mengembangkan kemampuan mereka untuk mengidentifikasikan, menggagalkan, dan melaporkan upaya rekaya sosial yang berbahaya (Aldawood & Skinner, 2019).

Cara pencegahan terbaik terhadap serangan rekayasa sosial adalah melalui edukasi dan kesadaran. Metode edukasi yang berpotensi antara lain metode penyampaian secara daring melalui penyebaran email, media sosial, diskusi daring, blog; metode penyampaian berbasis permainan yang memberikan tantangan, motivasi, dan keterikatan anggota-anggota dalam sebuah organisasi; metode berbasis video dan pembelajaran mandiri yang memungkinkan orang belajar mandiri; metode penyampaian berbasis simulasi seperti simulasi *email phishing* untuk menilai kelemahan pengguna dan mengukur tingkat kesadaran pengguna (Aldawood & Skinner, 2018).

Kegiatan Pengabdian kepada Masyarakat (PkM) ini bertujuan untuk meningkatkan literasi digital masyarakat terhadap *social engineering*, melalui edukasi kepada masyarakat dengan menggunakan metode berbasis video dan disampaikan secara daring. Dan dengan adanya

edukasi melalui kegiatan PkM ini, peningkatan pengetahuan dan kesadaran masyarakat terhadap *social engineering* adalah manfaat yang dapat dirasakan oleh masyaraka, sehingga masyarakat pada akhirnya tidak menjadi korban dari kejahatan siber.

## METODE

Dalam pelaksanaan PkM ini dilakukan beberapa tahapan untuk mencapai tujuan, seperti ditunjukkan gambar 3, yang meliputi 1) studi literatur terkait *social engineering*; 2) pembuatan video *social engineering*; 3) pembuatan kuesioner untuk mengetahui demografi dan tingkat kesadaran masyarakat baik sebelum maupun sesudah menonton video edukasi mengenai *social engineering* dan upaya mitigasinya; 4) distribusi video dan kuesioner yang dilakukan secara daring dengan menyebarkan *link* kuesioner melalui media sosial whatsapp; 5) analisis terhadap hasil kuesioner yang telah diisi oleh partisipan; dan 6) penarikan kesimpulan apakah ada peningkatan literasi digital masyarakat terhadap *social engineering*.


Gambar 3. Tahapan Pelaksanaan PkM

Studi literatur dilakukan untuk mendapatkan ragam aktivitas *social engineering* beserta mitigasinya sebagai bahan konten dari pembuatan video edukasi. Setelah itu, 3 video edukasi dibuat. Selain itu, dengan menggunakan google form, kuesioner dibuat untuk mengetahui tingkat pengetahuan dan kesadaran masyarakat sebelum dan sesudah menonton video edukasi Kemudian video edukasi dan kuesioner didistribusikan ke partisipan. Dalam mendapatkan partisipan di dalam kegiatan ini digunakan teknik *sampling snowball*, yaitu partisipan akan merekomendasikan ke partisipan berikutnya untuk mengisi kuesioner ini (Nurdiani, 2014). Hasil dari kuesioner ini kemudian dianalisis sebagai dasar penarikan kesimpulan, apakah ada peningkatan literasi digital khususnya mengenai *social engineering.*

## HASIL DAN PEMBAHASAN

### 1. Pembuatan Video

Dalam pembuatan video, dilakukan studi literatur terlebih dahulu mengenai aktivitas *social engineering* yang sering terjadi. Dalam studi yang dilakukan Lallie et al. (2021) kategori *phising* menempati persentase tertinggi dari kategori kejahatan siber pada masa pandemi COVID-19 ini. Oleh karena itu, *email phising* dan *vishing* dipilih sebgai konten video edukasi dalam kegiatan PkM ini.

Gambar 4. Video Edukasi : *Email Phising*

Video yang dibuat digunakan sebagai metode edukasi bagi masyarakat mengenai berbagai metode dalam *social engineering* dan bagaimana upaya pencegahan ataupun mitigasi terhadap aktivitas *social engineering* tersebut. Ada 3 video yang dibuat di sini, yaitu mengenail *email phising* ( gambar 4), *vishing* yang ditujukan kepada masyarakat umum (gambar 5), dan *vishing* yang target korbannya adalah personil perusahaan (gambar 6).

Di dalam video edukasi *email phising* ini dipaparkan karakteristik dari *email phising*. Melalui karakteristik tersebut, masyarakat dapat mengidentifikasikan apakah sebuah email merupakan *email phising* atau bukan. Selain itu, di dalam video ini juga diberikan upaya pencegahan maupun mitigasi terhadap *email phising* ini sehingga masyarakat dapat berhati-hati dan dapat melakukan antisipasi untuk tidak jatuh ke dalam jebakan yang diberikan oleh pelaku kejahatan melalui email ini.


Gambar 5. Video Edukasi : *Vishing*

Gambar 6. Video Edukasi : *Vishing* Perusahaan

*Vishing* singkatan dari *voice phising*, merupakan salah satu metode dalam *social engineering* yang banyak digunakan oleh penjahat siber. Dengan menirukan suara, penjahat mencoba menipu dan mengambil keuntungan dari si korban. Video edukasi ke-2 mengenai *vishing* ini dibuat dengan menggunakan skenario kejadian yang banyak terjadi. Kepanikan seorang ibu mendengar anaknya kecelakaan dan dirawat di rumah sakit dimanfaatkan oleh si pelaku untuk mendapatkan uang.

*Vishing* juga sering menargetkan sebuah perusahaan untuk mendapatkan keuntungan yang sebesar-besarnya. Skenario penipuan dengan meniru suara dan menjadikan sebuah perusahaan sebagai target korban menjadi konten video edukasi yang ke-3. Upaya dan mitigasi juga diberikan di akhir skenario cerita sebagai upaya meningkatkan kesadaran personil perusahaan.

Ketiga video yang telah dibuat kemudian diunggah ke channel youtube sehingga masyarakat dapat mengaksesnya dengan mudah, bahkan nantinya diharapkan masyarakat dapat membagikan video edukasi tersebut kepada kerabat, relasi, dan teman sehingga dampak positif yang dirasakan dapat meluas.

**2. Pembuatan kuesioner**

Setelah pembuatan video selesai, dilanjutkan ke pembuatan kuesioner. Kuesioner dibuat menggunakan google form. Demografi partisipan meliputi jenis kelamin, tingkat pendidikan, area pendidikan, dan jenis pekerjaan menjadi pertanyaan awal pada kuesioner ini. Link video edukasi dimasukkan sekaligus ke dalam kuesioner ini, sehingga partisipan dipastikan akan menonton video tersebut. Pertanyaan sebelum dan sesudah video disusun untuk mengetahui pengetahuan dan kesadaran masyarakat akan *social engineering.*

Tabel 1. Demografi Partisipan

| | | |
|---|---|---|
| Jenis Kelamin | Laki-laki | 51% |
| | Perempuan | 49% |
| Tingkat Pendidikan | SD, SMP, SMA, SMK | 21% |
| | Diploma | 10% |
| | S1 | 63% |
| | S2 | 6% |
| Area Pendidikan | IT | 29% |
| | Non-IT | 71% |
| Jenis Pekerjaan | Pelajar / Mahasiswa | 18% |
| | PNS | 2% |
| | Pegawai Swasta/Wiraswasta | 60% |
| | Ibu Rumah Tangga | 13% |

| | | |
|---|---|---|
| | Lain-lain | 7% |

**3. Distribusi video dan kuesioner**

Video dan kuesioner yang dikemas dalam satu form, didistribusikan secara daring kepada masyarakat melalui media sosial whatsapp dengan membagikan link menuju google form kuesioner tersebut. Pemilihan partisipan awal disesuikan dengan konten video edukasi, misal untuk video ke-3, yang berisi skenario *vishing* dengan target korban adalah sebuah perusahaan, maka partisipan yang dipilih adalah partisipan yang bekerja di perusahaan.

Melalui distribusi secara daring, diperoleh 68 partisipan dengan berbagai macam demografi, seperti jenis kelamin, tingkat pendidikan, area pendidikan, dan jenis pekerjaan yang ditunjukkan pada Tabel 1.

Dari 68 partisipan, mayoritas partisipan, yaitu 71%, tidak memiliki latar belakang pendidikan IT. Dan dari kuesioner yang diberikan sebelum menonton video edukasi, sebagian besar partisipan belum mengetahui metode-metode dalam *social engineering.*

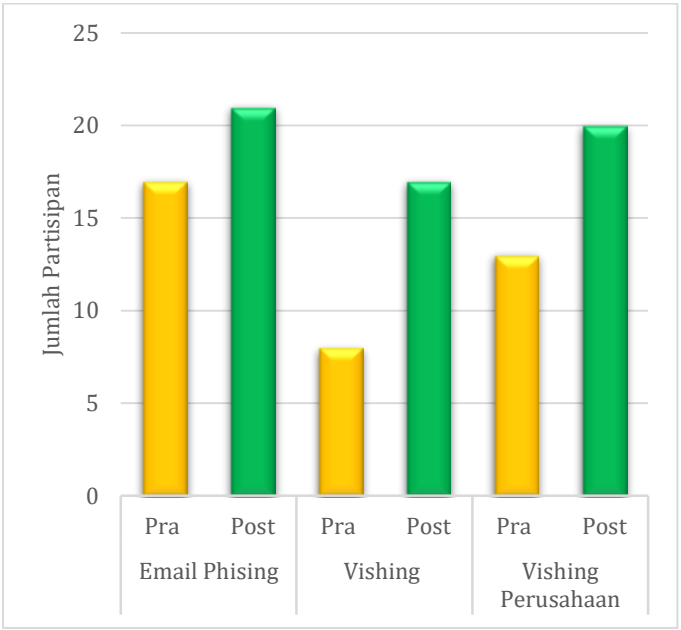
**4. Analisis hasil kuesioner**

Setelah video edukasi ditonton, partisipan diminta mengisi kuesioner untuk mengetahui peningkatan kesadaran masyarakat terhadap *social engineering*. Dari setiap jenis video, diperoleh hasil seperti yang ditunjukkan pada Tabel 2, bahwa pada *email phising*, 71% partisipan dapat mengidentifikasikan *email phising* dan 95% partisipan memiliki kesadaran untuk berhati-hati terhadap *email phising*. Pada video ke-2, yaitu v*ishing*, setelah partisipan menonton video tersebut diperoleh 82% partisipan dapat mengidentifikasikan *vishing* dan 100% partisipan sadar untuk berhati-hati terhadap *vishing* dengan memastikan kebenaran informasi. Sedangkan video ke-3, partisipan yang ditargetkan adalah partisipan yang bekerja pada perusahaan. Dari hasil kuesioner setelah menonton video, diperoleh 80% partisipan mampu mengidentifikasikan *vishing* dan 96% partisipan sadar untuk berhati-hati terhadap *vishing*.

Dari ketiga video tersebut terlihat bahwa persentase yang dicapai lebih dari 70%. Hal ini menunjukkan bahwa persentase masyarakat yang memiliki kesadaran terhadap *social engineering* setelah menonton video edukasi cukup banyak.

Tabel 2. Hasil Kuesioner Setelah Edukasi

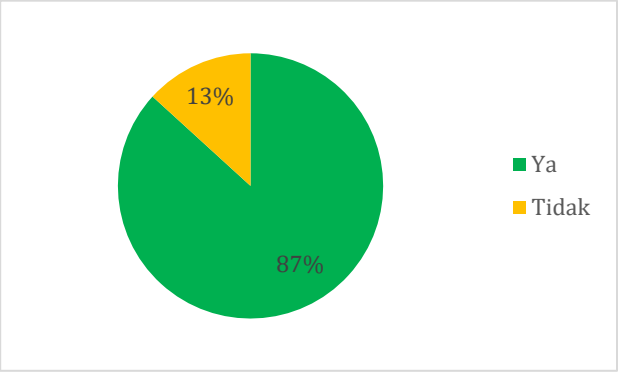
| | | |
|---|---|---|
| *Email Phising* | Identifikasi | 71% |
| | Antisipasi | 95% |
| *Vishing* | Identifikasi | 82% |
| | Antisipasi | 100% |
| *Vishing* Perusahaan | Identifikasi | 80% |
| | Antisipasi | 96% |




Gambar 7. Peningkatan Kesadaran Masyarakat terhadap *Social Engineering*

Untuk mengetahui peningkatan literasi digital masyarakat terhadap *social engineering* ini maka hasil kuesioner sebelum (pra) dan sesudah (post) partisipan menonton video edukasi dibandingkan. Gambar 7 menunjukkan hasil kuesioner pra dan post untuk setiap jenis video

edukasi. Dari setiap video dapat dilihat ada peningkatan. Pada video edukasi *email phising*, peningkatan hanya sekitar 23.53%. Sedangkan pada video *vishing* terjadi peningkatan secara signifikan, yaitu 112.50%. Peningkatan yang terjadi pada video *vishing* yang ditargetkan untuk perusahaan mencapai sekitar 53.85%. Sehingga diperoleh rata-rata persentase peningkatan dari ketiga video tersebut adalah 63.29%




Gambar 8. Manfaat PkM Bagi Masyarakat

Di akhir kuesioner, diberikan pertanyaan kepada partisipan untuk mengetahui apakah kegiatan PkM melalui video edukasi untuk meningkatkan literasi digital terhadap *social engineering* ini bermanfaat dan apakah mereka mau meneruskan video tersebut kepada relasi, kerabat, atau teman. Dari 68 partisipan, seperti terlihat pada gambar 8, 87% partisipan merasa bahwa PkM ini bermanfaat dan bersedia meneruskan kuesioner tersebut ke relasi, kerabat, dan teman, sedangkan sisanya 13% tidak bersedia meneruskan survey tersebut.

Dari hasil kuesioner dapat dilihat bahwa dampak dari kegiatan PkM ini meningkatkan literasi digital masyarakat mengenai *social engineering*.

Kegiatan peningkatan literasi digital memerlukan proses yang panjang, sehingga kegiatan ini dapat dilanjutkan secara bersikenambungan dengan membuat platform untuk mengunggah video edukasi sehingga masyarakat dapat mengaksesnya kapan saja dan dari mana saja sehingga dampaknya lebih meluas.

## KESIMPULAN

Kegiatan PkM yang ditujukan untuk meningkatkan literasi digital masyarakat terhadap *social engineering* melalui pembuatan video edukasi ini telah memberikan manfaat. Hal ini dapat dilihat dari peningkatan hasil identifikasi masyarakat terhadap aktivitas *social engineering* setelah melihat video edukasi, dengan rata-rata persentase kenaikan adalah 63.29%. Sebanyak 87% partisipan juga setuju bahwa kegiatan ini bermanfaat dan mau meneruskan video edukasi beserta kuesioner kepada relasi, kerabat, dan teman-temannya. Diharapkan dengan semakin banyaknya masyarakat yang menonton video edukasi, maka semakin meningkat pula literasi digital masyarakat terhadap *social engineering*. Sehingga pada akhirnya jumlah kejahatan siber di Indonesia dapat diminimalisir.

## REFERENSI

Aldawood, H., & Skinner, G. (2018). Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018. Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018, December, 62–68. https://doi.org/10.1109/tale.2018.8615293

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. Future Internet, 11(3). https://doi.org/10.3390/fi11030073

Arianto, A. R., & Anggraini, G. (2019). Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team on Internet Infrastructure (Id-Sirtii). Jurnal Pertahanan & Bela Negara, 9(1),13. https://doi.org/10.33172/jpbh.v9i1.497

Bakhshi, T. (2018). Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. Proceedings - 2017 13th International Conference on Emerging Technologies, ICET2017, 2018-Janua, 1–6. https://doi.org/10.1109/ICET.2017.8281653

Hadi, M. D. S., Widodo, P., & Putro, R. W. (2020). Analisis dampak pandemi Covid 19 di Indonesia ditinjau dari sudut pandang keamanan Siber. Jurnal Kebangsaan, 1(1), 1–9.

Ikhsan, M. (2020). BSSN Sebut Keamanan Siber RI 2020 Naik, Serangan Meningkat. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20200925104631-185-550825/bssn-sebut-keamanan-siber-ri-2020-naik-serangan-meningkat

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers and Security, 105, 1–20. https://doi.org/10.1016/j.cose.2021.102248

Nurdiani, N. (2014). Teknik Sampling Snowball dalam Penelitian Lapangan. ComTech: Computer, Mathematics and Engineering Applications, 5(2), 1110. https://doi.org/10.21512/comtech.v5i2.2427

Salsabila, P. Z. (2020). Kejahatan Siber di Indonesia Naik 4 Kali Lipat Selama Pandemi. Kompas.Com. https://tekno.kompas.com/read/2020/10/12/07020007/kejahatan-siber-di-indonesia-naik-4-kali-lipat-selama-pandemi

Tobing, V. (2020). Insiden web defacement. Juni 2020(Maret), 4–5. https://bssn.go.id/rekap-serangan-siber-januari-april-2020

Wicaksana, R. H., Munandar, A. I., & Samputra, P. L. (2020). Studi Kebijakan Perlindungan Data Pribadi dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi COVID-19. Jurnal IPTEK-KOM, 22(2), 143–158. https://jurnal.kominfo.go.id/index.php/iptekkom/article/download/3505/1477

.