Perwira Journal of Community Development
Vol.3 (No. 2) 2023, 29-34
ISSN Online 2798-3706

EDUKASI KEAMANAN DIGITAL MENGGUNAKAN APLIKASI GETCONTACT PADA MASYARAKAT DESA PANONGAN LOR

Indra Surya Permana[1], Carolus Borromeus Krishna Sampurno2, Rivanni Putri Ramadhini[3]
[1,3] Program Studi Akuntansi, Fakultas Ekonomi, Universitas Nahdlatul Ulama Cirebon
[2] Program Studi Teknik Mesin, Fakultas Sains dan Teknik, Universitas Perwira Purbalingga

Penulis Korespondensi : Rivanni Putri Ramadhini (e-mail: Rivanniputrir26@gmail.com)

ABSTRAK

Banyak upaya untuk yang perlu dilakukan terkait pengembangan suatu usaha dalam peningkatan laba usaha UMKM. Penerapan strategi marketing dan pengelolaan sumberdaya manusia menjadi pilihan untuk pencapaian tujuan yang dinginkan. Strategi marketing produk dalam hal ini dijelaskan sebagai uraian rencana secara rinci yang berisikan tentang bagaimana cara mengenalkan maupun menjual sebuah produk yang bisa menarik konsumen potensial menjadi konsumen riil. Upaya ini dilakukan untuk memastikan bagaimana sebuah produk dapat dipasarkan secara efektif kepada satu target pasar tertentu. Sedangkan pengelolaan sumberdaya manusia dalam pembagian tugas yang jelasakan menghasilkan output yang lebih optimal karena adanya speialisasi kerja.

Kata Kunci : Strategi Marketing, Pengelolaan Sumberdaya Manusia

1. PENDAHULUAN

Teknologi yang semakin pesat berkembang diiringi juga dengan canggihnya kejahatan siber (*Phishing, Smishing, dan Vhising*) yang menyerang para pengguna teknologi [1]. Para korban dari kejahatan siber berasal dari masyarakat umum hingga para profesional yang memiliki profesi yang berkaitan dengan bidang keamanan. Modus kejahatan yang cukup sering menggunakan modus penipuan yang dilakukan melalui telepon yang mengatasnamakan suatu lembaga untuk meminta kode *One Time Password* (OTP) atau *Personal identification Number* (PIN). Menurut Federal Trade Commision (FTC), kasus penipuan tertinggi mencapai 31% dari 498.000 kasus dengan total kerugian mencapai 436 juta dolar [2]. Selama tahun 2021, Kementrian Kominfo telah menerima kasus laporan aduan sebanyak 115.756 di media sosial dan *e-commerce* [3].

Di tahun 2022 ini, ketika semakin canggih peralatan – peralatan elektronik masyarakat juga semakin mudah untuk mengakses internet. Dahulu, hanya masyarakat yang berada di kota - kota besar saja yang dapat mengakses internet dikarenakan keterbatasan sinyal dan kurangnya pengetahuan tentang teknologi di daerah pedesaan. Sekarang, baik di pedesaan maupun perkotaan masyarakat kalangan muda, tua, dan bahkan sampai anak – anak mampu menggunakan internet untuk berbagai macam hal sehingga semakin maraknya kasus penipuan online.

Penipuan online dapat diartikan sebagai suatu kejahatan, karena tindakan tersebut dapat merugikan seseorang dan memiliki sanksi hukuman yang jelas bagi pelakunya [4]. Banyak faktor yang menyebabkan terjadinya penipuan, faktor ekonomi dan lingkungan menjadi penyebab utama. Selain itu minimnya pelaku yang tertangkap pihak berwajib menyebabkan banyak bermunculan pelaku – pelaku lain yang hanya coba – coba.

Penipuan yang dilakukan di dunia maya, harus menjadi perhatian karena tindakan tersebut memiliki pengaruh yang sangat besar bagi kehidupan sosial korban dan diperlukan pencegahan karena media sosial sudah menjadi bagian dari kehidupan sehari-hari [5]. Terjadinya peristiwa penipuan dalam media sosial menunjukan bahwa tindakan pelaku penipuan memanfaatkan kepercayaan yang diberikan oleh korban dalam mempersepsi tawaran yang diberikan

Perwira Journal of Community Development
Vol.3 (No. 2) 2023, 29-34
ISSN Online 2798-3706

oleh pelaku saat interaksi berlangsung dan berita – berita yang memberikan hal – hal yang membuat korban percaya dengan hal tersebut. Umumnya sasaran korban adalah masyarakat yang baru bergabung menggunakan teknologi pada masa kini seperti HP dan ikut serta dalam kegiatan sosial media (facebook, whatsapp, instagram, dsb).

Internet telah menjadi bagian dari kehidupan kita sehari - hari. Dengan kemajuan teknologi yang pesat, banyak jenis penipuan yang muncul yang dilakukan secara online untuk mencari, mendapatkan data rahasia, dan menggunakannya untuk keuntungan pribadi. Berbagai jenis penipuan online yang telah muncul antara lain *Phishing, Smishing, dan Vhising* [6], [7].

Phishing adalah upaya penipuan untuk mendapatkan informasi atau data sensitif, seperti nama lengkap, password, dan informasi kartu kredit/debit, dan lainnya, melalui media elektronik dengan menyamar sebagai sosok/pihak yang dapat dipercaya. Pelaku akan mengirimkan e-mail yang mengatasnamakan pihak tertentu dan memancing korban untuk mengeklik link yang tercantum di dalam e-mail. Semua untuk mendorong korban bertindak sesuai dengan yang pelaku harapkan.

Smishing adalah penipuan Dengan mengetahui nomor handphone kamu, pelaku bisa mengirimkan pesan/SMS mengatasnamakan pihak terpercaya yang bertujuan untuk mengelabui kamu supaya mengeklik link berbahaya berisi malware atau mengarahkanmu ke website buatan pelaku.

Voice phishing atau ***vhishing*** adalah bentuk penipuan melalui telepon. Penipu menggunakan social engineering melalui telepon untuk mendapatkan akses ke informasi dan keuangan pribadi kamu. Sama seperti phishing dan smishing, korban akan diiming-imingi hadiah atau menerima desakan untuk memberikan data pribadi jika tidak ingin hal yang gak diharapkan terjadi.

Saat ini banyak sekali informan yang memberikan informasi dengan kreatifitas yang mudah di pahami oleh masyarakat dan dapat di aplikasikan oleh masyarakat dengan mudah. Informasi yang diberikan tentang apa saja bentuk – bentuk penipuan yang ada saat ini dengan menggunakan istilah – istilah yang mudah di pahami masyarakat dan dengan istilah yang terus berkembang seiring dengan kemunculan berbagai bentuk penipuan online. Aksi kejahatan ini tidak dapat dihindari dari kemajuan teknologi pada masa kini yakni dengan kemajuan teknologi industri 4.0.

Istilah Industry 4.0 pertama kali digemakan pada Hannover Fair, 4-8 April 2011. Istilah ini digunakan oleh pemerintah Jerman untuk memajukan bidang industri ke tingkat selanjutnya, dengan bantuan teknologi komputer. pelaku industri membiarkan komputer saling terhubung dan berkomunikasi satu sama lain untuk akhirnya membuat keputusan tanpa keterlibatan manusia. Kombinasi dari sistem fisik-*cyber*, Internet of Things (IoT), dan Internet of Systems membuat Industry 4.0 menjadi mungkin, serta membuat pabrik pintar menjadi kenyataan. Di Indonesia, perkembangan Industry 4.0 sangat didorong oleh Kementerian Perindustrian. Menteri Perindustrian Airlangga Hartarto mengatakan, agar Indonesia dapat bersaing dengan negara lain di bidang industri, Indonesia juga harus mengikuti tren dengan mengikuti perkembangan zaman [8].

UUD 1945 pasal 378 KUHP berbunyi "Barangsiapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang, diancam karena penipuan dengan pidana penjara paling lama empat tahun" dengan ancaman Hukuman maksimal 4 tahun penjara. Sedangkan untuk mengatur tentang aktifitas transaksi online di Indonesia dan memberikan pembaruan hukum dengan tujuan menjamin kepentingan masyarakat akan jaminan kepastian hukum untuk bertransaksi dengan memanfaatkan media elektronik diatur dalam UU ITE [9].

Sebagian besar penduduk Desa Panongan Lor, Kabupaten Cirebon, Jawa Barat ini berprofesi sebagai petani, buruh tani, dan ibu rumah tangga. Sehingga mereka menggunakan HP hanya pada saat waktu senggang sebelum istirahat bahkan hanya digunakan untuk melakukan komunikasi dengan sanak saudara dan hal – hal yang menyangkut pada pekerjaan. Sedangkan, untuk anak remaja digunakan untuk beberapa hal seperti mencari berbagai informasi dengan aplikasi pencarian (Google), game online, melakukan komukasi, dan mencari hiburan (aplikasi tiktok, snack video, instagram, dll).

Kegiatan ini difokuskan untuk program bidang teknologi dan informasi ini dengan pengembangan dan peningkatan pemahaman masyarakat pada ranah kejahatan online yang dilakukan oleh oknum – oknum yang tidak bertanggung jawab. Alasan mengapa harus dilakukannya peningkatan pemahaman dan pencegahan karena pernah terjadinya warga yang terjebak oleh tipuan kejahatan yang beredar agar tidak ada lagi korban. Beberapa warga Desa Panongan Lor ada yang pernah terjebak oleh kejahatan ini salah satunya dengan mengklik situs link yang dikirimkan melalui whatsapp, dan sms hingga pernah melakukan transaksi atau mengirimkan uang untuk sang penipu dengan jumlah Rp. 500.000.

2. METODE

Perwira Journal of Community Development
Vol.3 (No. 2) 2023, 29-34
ISSN Online 2798-3706

Metode yang digunakan untuk mencapai tujuan yaitu menggunakan metode analisis deskriptif yang bertujuan untuk memberikan deskripsi atau gambaran mengenai subjek penelitian berdasarkan data atau informasi yang diperoleh.

Pada kegiatan ini juga menggunakan metode wawancara sehingga menimbulkan pertanyaan yang perlu di jawab :

A. Apa yang dimaksud dengan bermedia digital ?
B. Mengapa penting melakukan proteksi perangkat digital ?
C. Bagaimana cara melakukan proteksi perangkat digital?
D. Bagaimana cara agar kita aman bermedia digital ?
E. Bagaimana cara melindungi data pribadi di platform digital ?

Setelah dilakukan wawancara pada masyarakat, kemudian dapat diambil kesimpulan masalah – masalah yang dihadapi penduduk panongan lor mengenai teknologi digital. Berdasarkan masalah tersebut, kemudian dilakukan sosialisasi mengenai teknologi digital melalui tahapan sebagai berikut :

a) Analisis situasi dan studi kelayakan yang terkait dengan kurangnya pemahaman masyarakat tentang literasi digital.
b) Identifikasi kebutuhan dan permasalahan yang berkaitan dengan literasi digital.
c) Perencanaan program sosialiasi berupa pembekalan mahasiswa dan implementasi literasi digital.

Pelaksanaan kegiatan kemudian dibagi menjadi empat tahapan, yaitu :

a) Tahap Training of Trainer TOT di lokasi KKN untuk sosialisasi dan pemberian pengetahuan tentang Literasi Digital tentang bagaimana menggunakan internet dan teknologi dengan memberikan pengetahuan kepada masyarakat tentang Keamanan Digital, Etis Digital, Cakap Digital, dan Budaya Digital.
b) Tahap sosialisasi di lapangan dengan memberikan materi dan memberikan contoh menggunakan alat peraga (Handphone).
c) Tahap evaluasi program untuk perbaikan dan perencanaan tindak lanjut.

3. HASIL

Kegiatan KKN UNU yang berupa pengabdian kepada masyarakat ini diawali dengan dilakukannya observasi dan analisis di daerah tempat KKN pada tanggal 15 Agustus 2022. Kemudian pada tanggal 20 Agustus 2022 dilakukan pertemuan dan sosialisasi tentang masalah – masalah yang terdata dan juga menambahkan tentang 4 pilar literasi digital pada masyakat Desa Panongan Lor blok simbar dengan memaparkan materi dan memberikan contoh dengan alat peraga kepada masyarakat agar lebih mudah memahami.

Gambar 4. Pemberian Materi menggunakan alat peraga

Kegiatan sosialisasi difokuskan pada materi keamanan bermain digital sesuai dengan modul materi yang telah diberikan oleh pihak kampus, yang kemudian di paparkan kembali pada warga. Berikut jawaban dari pertanyaan yang ada pada bagian metode :

a) Bermedia digital adalah proses memastikan penggunaan layanan digital dapat dilakukan secara aman dan nyaman baik secara daring maupun luring.
b) Pentingnya melakukan proteksi perangkat digital
   - Agar orang yang tidak bertanggung jawab tidak dapat mencuri informasi pribadi milik kita atau uang kita.
   - Mencegah terjadinya pengambilan dan pencurian data penting yang kita miliki.
   - Perangkat digital sering menjadi incaran upaya peretasan.
   - Banyak pengguna lalai dan lupa mengaktifkan fitur pengaman.
c) Cara melakukan proteksi perangkat digital

Tabel 1. Jenis proteksi perangkat

Proteksi Perangkat Keras	Proteksi Perangkat Lunak
▪ Menggunakan fitur kata sandi ▪ Menggunakan fitur *Fingerprint Authentication* ▪ Menggunakan fitur *Face Authentication*	▪ Menggunakan fitur *Find My Device* ▪ Memahami dan melindungi data dengan fitur *Back-up data* ▪ Menggunakan fitur enkripsi *full disk* ▪ Menggunakan fitur *shredder*

d) Cara aman bermedia digital

Perwira Journal of Community Development
Vol.3 (No. 2) 2023, 29-34
ISSN Online 2798-3706

Gambar 1. Langkah aman dalam bermedia digital.

e) Cara melindungi data pribadi di platform digital

Data pribadi adalah Identitas seseorang sebagai pengguna platform media digital (Monggilo, Kurnia, & Banyumurti 2020).

Data terbagi menjadi data pribadi umum dan data pribadi khusus :

Tabel 2. Jenis data pribadi

Data Pribadi Umum	Data Pribadi Khusus
♦ Nama	♦ Data Kesehatan
♦ Jenis Kelamin	♦ Biometrik Genetika
♦ Kewarganegaraan	♦ Keuangan
♦ Agama	♦ Ras/Etnis
♦ Tanggal Lahir	♦ Data Keluarga
♦ Pekerjaan	♦ Preferensi Seksual
♦ Alamat Rumah	♦ Pandangan Politik
♦ E-mail	♦ Data Kejahatan
♦ Nomor	
♦ Telepon	

Dari data – data tersebut yang harus dilakukan untuk menjaga data pribadi kita yaitu dengan cara :

1) Gunakan password (sandi) yang sulit dan gunakan sandi yang secara berbeda di setiap akun sosial medial yang dimiliki.
2) Pahami dan pastikan pengaturan privasi di setiap akun platform digital yang dimiliki sesuai dengan tingkat keamanan yang dibutuhkan.
3) Pastikan memilih menggunakan identitas asli atau samaran saat mengelola akun platform digital serta bertanggungjawab atas pilihan tersebut.
4) Jangan membagikan data pribadi kita (tempat tanggal lahir, nama ibu kandung, password berbagai akun platform digital).
5) Jangan memberikan data pribadi orang lain baik keluarga, teman, maupun kenalan di dunia maya sebab data mereka adalah privasi.
6) Hindari memasukkan data pribadi yang penting saat berinteraksi dalam platform digital dengan menggunakan Wi-Fi gratis di tempat publik.
7) Pahami dan pilih aplikasi yang dipasang yang hanya mengakses data yang dibutuhkan, bukan data pribadi kita lainnya.
8) Selalu lakukan pembaruan perangkat lunak yang digunakan untuk meminimalisir resiko ada celah kebocoran.
9) Waspada jika ada komunikasi atau aktivitas mencurigakan dari akun yang kita kenal ataupun yang tidak kita kenal.

f) Perlindungan identitas Digital di Platform Digital

Tabel 3. Jenis identitas digital

Identitas yang terlihat	Identitas tidak terlihat
▪ Nama Akun	▪ PIN/Password/Sandi
▪ Foto Profil Pengguna	▪ *Two Factor Authentication*
▪ Deskripsi Pengguna	▪ OTP
▪ Identitas Lain yang Tercantum Dalam Akun	▪ Identitas Lain

Langkah – langkah melindungi identitas digital

1) Pastikan memilih menggunakan identitas asli atau samaran saat mengelola akun platform digital serta bertanggungjawab atas pilihan tersebut.
2) Amankan identitas utama yakni alamatsurat elektronik (surel) yang kita gunakan untuk mendaftar suatu platform digital.
3) Lindungi dan konsolidasikan identitas digital dalam berbagai platform digital yang dimiliki.

g) Fitur yang dapat melindungi data pribadi pada perangkat

1) PIN
PIN adalah angka sandi yang hanya diketahui oleh pengguna dan sistem autentikasi platform digital tersebut . Biasanya PIN terdiri dari 4 hingga 6 digit angka yang digunakan sebagai cara sistem melakukan identifikasi terhadap pengguna agar akses ke sistem tersebut terbuka dan pengguna bisa memanfaatkan aneka fitur dan layanan dalam platform digital.

2) OTP (One Time Password)
Penggunaan kode unik yang khas dan difungsikan satu kali dalam satu transaksi

3) 2FA
2FA adalah fitur keamanan yang digunakan untuk melakukan autentikasi ulang apakah pengguna yang akan login adalah benar-benar pemilik akun tersebut benar dan terdaftar dalam sistem.

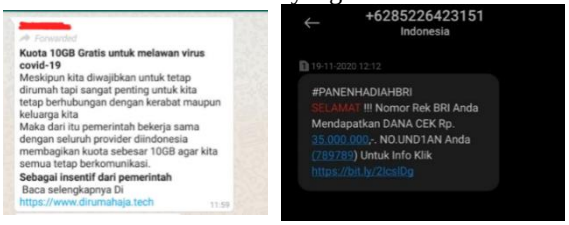
Tahapan dan Hasil Sosialisasi Pengembangan dan Peningkatan Pemahaman Masyarakat Pada Ranah Kejahatan Online

A. Tahapan Sosialisasi

Tahapan ini dilakukan pada tanggal 20 Agustus 2022 berupa sosialiasi dan wawancara serta

Perwira Journal of Community Development
Vol.3 (No. 2) 2023, 29-34
ISSN Online 2798-3706

memberikan solusi kepada warga agar tidak mudah tertipu oleh hal – hal kejahatan. Pada kegiatan ini diberikan materi – materi pemahaman tentang literasi digital dan bertanya pada warga tentang siapa yang pernah melakukan hal – hal yang disosialisasikan.



Gambar 2. Bukti kejahatan dan *phising* SMS

Setelah melakukan wawancara kepada warga, kemudian diberikan saran pada warga agar dapat mencegah aksi kejahatan tersebut dengan memperkaya diri akan informasi dan mengenali seputar hal –hal yang perlu kita hindari dari tindak penipuan tersebut, menjaga data diri, jangan sembarangan mengklik tautan, dan mempercayai nomor telepon yang menghubungi jika dirasa tidak mengenalnya.

Warga disarankan untuk menginstal aplikasi *Getcontact* sebagai tindakan mengurangi aksi penipuan dikarenakan aplikasi ini sangat mudah digunakan cukup mengunduh aplikasi *Getcontact* pada HP kita melalui Play Store untuk pengguna android atau App Store untuk pengguna iphone, kemudian pengguna hanya perlu verifikasi dengan masuk menggunakan nomor telepon pengguna. Jika sudah masuk kedalam aplikasi dan muncul tampilan aplikasi beri perizinan aplikasi untuk mengakses kotak anda dan kita dapat melihat juga tag nama kita pada HP orang lain.

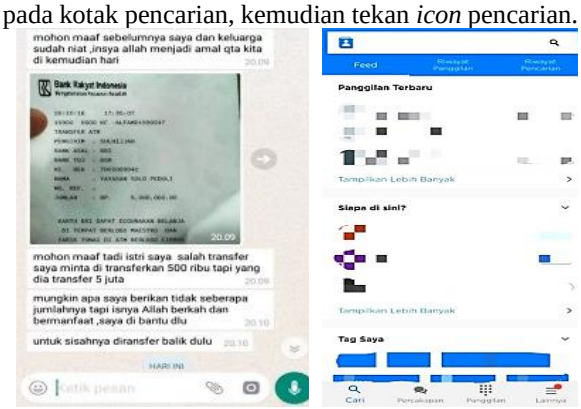
Gambar 3. Tampilan Aplikasi *Getcontact*

Kelebihan aplikasi *Getcontact* yaitu menyaring panggilan yang mengganggu atau nomor telepon yang tidak kita kenal dan hanya nomor telepon orang yang kita pilih saja untuk berkomunikasi dengan kita. Namun, aplikasi ini juga memiliki kelemahan yaitu tidak semua Hp dapat menggunakan aplikasi ini dan hanya dapat beroprasi pada Android dengan minimal versi android 4.0.3 (Ice Cream Sandwich) dan iOS.

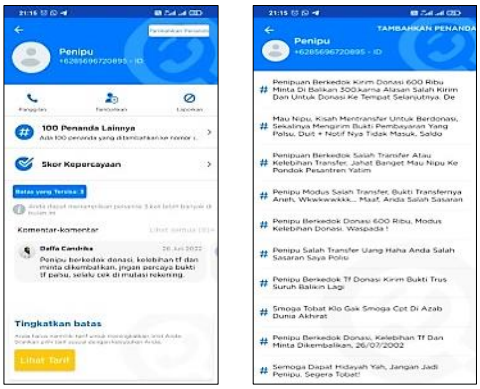
B. Kasus yang pernah dihadapi dan bagaimana memanfaatkan *Getcontact*

Pada saat menjalankan kegiatan pengabdian kepada masyarakat Desa Panongan Lor, Kecamatan Sedong, Kabupaten Cirebon. Kami membuka kepada warga media sosial untuk memberikan sumbangan (Donasi) yang akan diberikan diberbagai tempat yang ada di Desa Panongan Lor, Kecamatan Sedong, Kabupaten Cirebon. Terdapat masalah dalam kegiatan ini dikarenakan adanya kejahatan *cyber*. Berikut bukti dan cara menggunakan aplikasi *Getcontact*.

Masukan nomor telepon yang memberikan pesan pada kotak pencarian, kemudian tekan *icon* pencarian.



Gambar 5. Bukti pesan penipuan & tampilan aplikasi *Getcontact*



Gambar 6. Tampilan pencarian & identifikasi nomor pada aplikasi *Getcontact*

Seperti itulah cara penggunaan dan cara kerja aplikasi *Getcontact*. Kita dapat mengetahui nomor yang kita ragu. Tidak hanya melalui pesan tetapi juga dapat dicari jika ada penelepon yang mencurigakan maksud dan tujuan menghubungi

C. Hasil Sosialisasi

Pada kegiatan yang dilakukan dalam memberikan informasi kepada warga blok simbar telah diterima dengan baik dan dimengerti sehingga warga sudah dapat mengetahui hal – hal yang penting dalam bermedia digital dan mengoperasikan secara pribadi hal yang disampaikan dalam aspek keamaan berdigital agar tidak terjadinya aksi kejahatan pada warga. Warga menjadi semakin lebih baik dan lebih paham

Perwira Journal of Community Development
Vol.3 (No. 2) 2023, 29-34
ISSN Online 2798-3706

yang kemudian akan menjadi lebih pintar dalam bermedia digital.

4. KESIMPULAN

Setelah dilakukannya sosialisasi tentang literasi digital pada masyarakat Desa Panongan Lor blok simbar menjadikan warga Desa Panongan Lor, Kecamatan Sedong, Kabupaten Cirebon menjadi warga yang paham dan selektif dalam bermedia digital pada kehidupan sehari – hari, terutama pada aspek keamanan dalam bermedia digital. Warga menjadi paham dan mengerti cara menjadi keamanan data diri pada media digital. Betapa pentingnya dalam memahami dan informasi tentang aksi – aksi kejahatan online yang berada di sekeliling kehidupan kita dan cara menghindari aksi kejahatan sebagai antisipasi diri jika terjadi pada diri sendiri. Pada aksi kejahatan ini pelaku dapat dikenakan pasal 378 KUHP dengan ancaman hukuman maksimal 4 tahun penjara.

5. DAFTAR PUSTAKA

[1] D. N. Njuguna, J. Kamau, and D. Kaburu, "A Review of Smishing Attaks Mitigation Strategies," *Int. J. Comput. Inf. Technol.*, vol. 11, no. 1, 2022.

[2] F. T. Commision, "CSN Annual Data Book 2021," 2022. https://www.ftc.gov/system/files/ftc_gov/pdf/CSN Annual Data Book 2021 Final PDF.pdf

[3] C. Indonesia, "Kominfo Catat Kasus Penipuan Online Terbanyak : Jualan Online," 2021. https://www.cnnindonesia.com/teknologi/20211015085350-185-708099/kominfo-catat-kasus-penipuan-online-terbanyak-jualan-online

[4] A. Rusmana, "PENIPUAN DALAM INTERAKSI MELALUI MEDIA SOSIAL (Kasus Peristiwa Penipuan melalui Media Sosial dalam Masyarakat Berjejaring)," *J. Kaji. Inf. dan Perpust.*, vol. 3, no. 2, pp. 187–194, 2015.

[5] A. Buha, "Hubungan Subordinasi dan Semantis Dalam Kalimat Majemuk Bertingkat Bahasa Dayak Lundayeh," *J. Aksara*, vol. 29, no. 1, pp. 75–88, 2017.

[6] T. Guarda, M. F. Augusto, and I. Lopes, "The Art of Phishing," *Adv. Intell. Syst. Comput.*, vol. 918, pp. 683–690, 2019.

[7] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing , SMiShing & Vishing : An Assessment of Threats against Mobile Devices," *J. Emerg. Trends Comput. Inf. Sci.*, vol. 5, no. 4, pp. 297–307, 2014.

[8] K. K. dan I. RI, "Apa itu industri 4.0 dan bagaimana Indonesia menyongsongnya," 2019. https://www.kominfo.go.id/content/detail/16505/apa-itu-industri-40-dan-bagaimana-indonesia-menyongsongnya/0/sorotan_media

[9] A. Mu, G. Chintia, and P. N. Sari, "Edukasi Pencegahan Penipuan Online Berbasis Sosial Media di Desa Mekarwangi," vol. 3, no. 2, 2023.