Analisis Dan Mitigasi Ancaman *Social Engineering* Pada Pengguna Facebook Dengan Pendekatan OSINT

Rachman Nurhakim[1], Chairul Habibi[2], Marwondo[3]
Fakultas Teknologi dan Informatika
Universitas Informatika dan Bisnis Indonesia
Bandung, Indonesia
e-mail: [1]nurhakimg8888@gmail.com, [2]chairulhabibi@unibi.ac.id, [3]marwondo@unibi.ac.id

Correspondence : *e-mail*: nurhakimg8888@gmail.com

Diajukan: 30 Juli 2024; Direvisi: 20 Agustus 2024; Diterima: 20 Agustus 2024

Abstrak

Penelitian ini bertujuan untuk menganalisis dan memitigasi ancaman social engineering pada pengguna Facebook dengan pendekatan Open-Source Intelligence (OSINT), khususnya di Desa Bojong Emas RW 04. Dalam era digital yang semakin maju, media sosial seperti Facebook sering menjadi sasaran serangan social engineering yang bertujuan untuk mendapatkan informasi pribadi pengguna. Ancaman ini dapat menyebabkan berbagai kerugian, termasuk pencurian identitas dan penipuan finansial. Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus. Data diperoleh melalui observasi, serta analisis konten dari akun Facebook pengguna di Desa Bojong Emas RW 04. Penelitian ini juga memanfaatkan teknik OSINT untuk mengumpulkan dan menganalisis data yang tersedia secara publik di internet dan menggunakan taktik social engineering hingga tahap hook, guna mengidentifikasi potensi ancaman dan kelemahan dalam keamanan informasi pengguna. Hasil penelitian menunjukkan bahwa beberapa pengguna Facebook di Desa Bojong Emas RW 04 masih kurang menyadari bahaya social engineering dan sering mengabaikan langkah-langkah keamanan dasar seperti informasi pribadi yang tersebar luas. Berdasarkan temuan ini, penelitian ini mengembangkan beberapa rekomendasi mitigasi, termasuk edukasi keamanan siber, implementasi pengaturan privasi yang lebih ketat.

Kata kunci: *Social Engineering, Facebook, Open-Source Intelligence (OSINT), Keamanan Informasi*.

Abstract

This research aims to analyze and mitigate social engineering threats to Facebook users using Open-Source Intelligence (OSINT) approaches, specifically in Bojong Emas Village, RW 04. In the advancing digital era, social media platforms like Facebook are often targeted by social engineering attacks intended to obtain users' personal information. These threats can lead to various losses, including identity theft and financial fraud. This study employs a qualitative method with a case study approach. Data is collected through observation and content analysis of Facebook accounts belonging to users in Bojong Emas Village, RW 04. The research also utilizes OSINT techniques to gather and analyze publicly available data on the internet and employs social engineering tactics up to the hook stage to identify potential threats and weaknesses in users' information security. The findings reveal that some Facebook users in Bojong Emas Village, RW 04, are still unaware of the dangers of social engineering and often neglect basic security measures, such as widely disseminating personal information. Based on these findings, the study develops several mitigation recommendations, including cybersecurity education and the implementation of stricter privacy settings.

Keywords*: Social Engineering, Facebook, Open-Source Intelligence (OSINT), Information Security*.

1. Pendahuluan

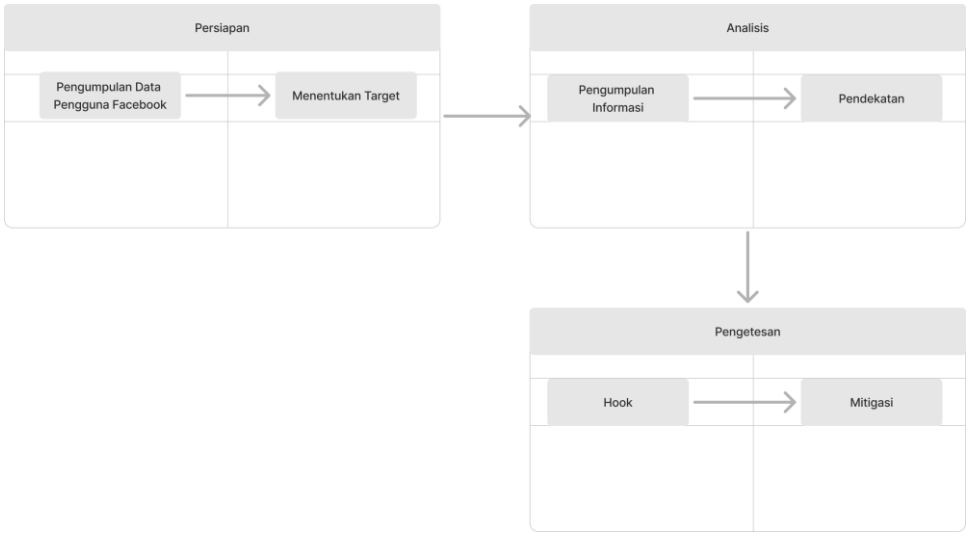
Seiring dengan meningkatnya pengguna internet di Indonesia yang mencapai 221.563.479 jiwa pada tahun 2024 [1], kasus serangan penipuan secara digital juga mengalami peningkatan, tercatat pada laporan bulan Januari 2024 dari Badan Siber dan Sandi Negara (BSSN) ada sebanyak 108 penipuan secara daring yang telah terjadi. Sedangkan pada Februari 2024 BSSN melaporkan telah terjadi 172 kejahatan siber meliputi penipuan secara daring yang dilaporkan ke BSSN [2][3], laporan tersebut berasal dari masyarakat yang menjadi korban penipuan secara daring. Kasus penipuan tersebut dapat terjadi di mana saja saat menjelajah internet, salah satunya pada media sosial Facebook, karena dengan kebiasaan pengguna

Facebook yang melakukan oversharing, dapat membuka peluang bagi para kriminal mencuri informasi pribadi yang bisa digunakan untuk mengeksploitasi korban [4]. Ancaman yang umum terjadi di Facebook adalah *social engineering* dan metode yang digunakan oleh pelaku *social engineering* diantaranya adalah *pretexting*, *spear phishing*, *phishing*, dan sebagainya [5].

Risiko ancaman *social engineering* tersebut dapat diminimalisir atau bahkan dicegah, dengan dilakukannya suatu analisis yang dapat digunakan untuk mengidentifikasi potensi risiko dan pola serangan yang mungkin terjadi [6][7]. Dengan menganalisis informasi publik yang tersedia secara daring, seperti profil pengguna, aktivitas daring, dan hubungan antar pengguna, dapat membantu dalam mengidentifikasi potensi celah keamanan dan memitigasi risiko serangan. Strategi mitigasi yang ada saat ini misalnya dari OJK yaitu penerapan strategi anti fraud [8], lebih dikhususkan kepada Bank Umum, kemudian panduan dari BSSN yaitu panduan penanganan *phishing* [9] masih kurang cukup sebab phishing sendiri memiliki banyak jenisnya, serta BSSN tidak menjelaskan pencegahan terhadap fase *Social engineering* yaitu fase yang paling krusial dalam penipuan secara daring.

Informasi pengguna yang tersedia pada Facebook bisa bersifat publik sehingga setiap informasi tersebut dapat dikategorikan sebagai *Open Source Intelligence* (OSINT). Penelitian ini menggunakan pendekatan OSINT karena cara tersebut lebih efektif digunakan untuk informasi yang bersifat publik dan tersedia secara daring, berbanding terbalik dengan *Human Intelligence* (HUMINT), yang lebih efektif untuk informasi lapangan secara langsung [10][11][12].

2. Metode Penelitian



Gambar 1. Alur Penelitian

2.1. Persiapan

Tahap penulis mengumpulkan informasi-informasi yang diperlukan untuk kepentingan penelitian. Pada tahap ini pengumpulan data dilakukan dengan melakukan studi literatur dan observasi. Data dikumpulkan melalui kegiatan pendataan secara langsung terhadap pengguna Facebook di Desa Bojong Emas RW 04 Kabupaten Bandung, data yang didapatkan berupa nama akun Facebook, profesi, dan rentang usia.

2.2. Analisis

Peneliti kemudian memulai proses pengumpulan data dengan mencari informasi yang dapat diakses secara bebas di internet, seperti profil media sosial, postingan publik, komentar, dan data lain yang relevan dengan target. Selama proses ini, peneliti menggunakan OSINT untuk mengidentifikasi jejak digital target, termasuk informasi pribadi yang mungkin tersebar di berbagai platform media sosial, situs web, dan forum. Data yang terkumpul kemudian diorganisir dan dikategorikan berdasarkan relevansi dan tingkat sensitivitasnya [13].

2.3. Pengetesan

Tahap ini dimulai dengan penyiapan skenario serangan yang realistis dan relevan dengan ancaman social engineering yang diidentifikasi pada tahap analisis. Skenario ini dirancang untuk mensimulasikan upaya penipuan atau manipulasi psikologis yang mungkin dilakukan oleh pelaku kejahatan siber terhadap pengguna Facebook di Desa Bojong Emas RW 04. Peneliti kemudian menggunakan teknik OSINT untuk

mengumpulkan informasi yang dibutuhkan untuk menjalankan skenario serangan tersebut. Informasi ini termasuk data pribadi, pola perilaku daring, dan interaksi sosial target yang sebelumnya diidentifikasi pada tahap analisis. Dengan informasi yang terkumpul, peneliti mencoba menguji kerentanan target melalui pendekatan social engineering hingga tahap 'hook'[14], di mana pelaku berusaha mendapatkan respons atau tindakan dari target yang mengarah pada kompromi keamanan. Selama proses pengetesan, peneliti memantau reaksi dan respon target terhadap skenario serangan. Hal ini melibatkan pengiriman pesan yang dirancang untuk memancing target mengungkapkan informasi sensitif atau melakukan tindakan tertentu yang berisiko.

.

3. Hasil dan Pembahasan

3.1. Pengumpulan Data

Total data yang penulis dapatkan berjumlah 289KK (Kepala Keluarga) dari 806 total jumlah penduduk, jumlah populasi ini diambil berdasarkan informasi yang diberikan oleh 5 (lima) RT (Rukun Tetangga) dari RW 04, dimana RT 01 berjumlah 63, RT 02 64, RT 03 58, RT 04 54, dan RT 05 50. Setelah penulis mendapatkan jumlah populasi yang ada maka berikutnya penulis menerapkan rumus Slovin untuk mendapatkan sampel yang dibutuhkan, dan hasilnya adalah sebagai berikut:

$$n = \frac{806}{1 + 806(0{,}1)^2}$$

$$n = \frac{806}{9{,}06}$$

$$n = 88{,}96$$

Jumlah sampel yang dibutuhkan adalah 88,96 (dibulatkan menjadi 90) dengan menghitung *margin of error* sebanyak 10%, *margin of error* ini penulis dapatkan dari beberapa penelitian lain dengan jumlah populasi yang tidak lebih dari 1000 maka *error* yang ditentukan adalah 10% [15]. Cara yang dilakukan penulis untuk pengambilan sampel adalah dengan langsung melakukan observasi dan survey.

3.2. Penentuan Target

Terdapat 5 kriteria yang dibuat oleh *Elevate Security* tentang hal yang dilihat oleh seorang peretas terhadap korbannya, yaitu:

1. Orang-orang yang memiliki akses langsung ke data rahasia, termasuk kode sumber (*engineers*).
2. Korban serangan *social engineering* biasanya memiliki tingkat risiko yang lebih tinggi dan lebih rentan terhadap serangan.
3. Individu yang memiliki banyak informasi yang dapat dikumpulkan melalui media sosial dan cara lain di internet.
4. Menargetkan karyawan baru yang mungkin belum sepenuhnya familiar dengan protokol keamanan perusahaan mereka.
5. Beberapa penyerang mungkin memanfaatkan penipuan malware untuk memancing dan menjebak korban.

Dari 90 akun yang ada, berikut adalah tabel yang menunjukkan jumlah akun yang memenuhi kriteria yang bisa dijadikan target serangan *social engineering*:

Tabel 1. Akun yang Memenuhi Kriteria

Kriteria	Jumlah Akun
1	1
2	0
3	79
4	1
5	-
Private	9

Hasilnya adalah 79 akun masuk ke dalam kriteria “Individu yang memiliki banyak informasi yang dapat dikumpulkan melalui media sosial dan cara lain di internet”. Semua 79 akun tersebut memiliki kerentanan yang hampir sama, diantaranya adalah sebagai berikut:

1. Akun dengan pengaturan privasi rendah yang menampilkan banyak informasi pribadi seperti alamat, nomor telepon, email, tanggal lahir, dan informasi keluarga.
2. Akun dengan jumlah teman atau koneksi yang tinggi, yang sering kali menandakan bahwa akun tersebut lebih mudah dipercaya oleh orang lain.
3. Akun yang sering membagikan secara mendetail dalam postingan atau status, seperti foto keluarga, lokasi saat ini, atau aktivitas sehari-hari, dan informasi pribadi.
4. Akun yang menunjukkan ketertarikan yang jelas pada produk, romansa, atau hobi tertentu, yang bisa dimanfaatkan untuk serangan yang lebih spesifik dan personal.

Berikut adalah tabel yang merangkum hasil pembagian akun berdasarkan kerentanannya:

Tabel 2. Hasil Pembagian Berdasarkan Kerentanan

Kerentanan	Jumlah Akun
1	36
2	3
3	0
4	1
1, 2	22
1, 3	3
2, 4	1
1, 2, 3	3
1, 3, 4	1
1, 2, 4	7
1, 2, 3, 4	1

Hasilnya adalah terdapat 79 akun yang terindikasi memiliki kerentanan terkait informasi pribadi, dengan total 74 akun yang informasi tanggal lahirnya terekspos.

3.3. Hook

Tujuan dari pendekatan awal ini adalah untuk memulai percakapan dan membuat target merasa nyaman. Pembangunan kepercayaan dilakukan dengan menunjukkan kesamaan, memberikan informasi yang bermanfaat, atau menunjukkan rasa peduli terhadap kebutuhan dan masalah target. Pengetesan dilakukan dengan menggunakan 2 cara, yaitu *direct message*, dan *friendly* dengan satu tujuan yang sama, yaitu untuk mendapatkan informasi lebih lanjut terkait target, terutama nomor kontak dan alamat tinggal, berikut adalah skenario yang penulis buat untuk melakukan pengetesan dengan menggunakan *direct message*, penulis menggunakan akun boneka untuk melakukan pengetesan dengan nama "Husnan Miftahul". Hasil dari skenario yang penulis buat dan melakukan pengetesan terhadap 74 akun adalah hanya ada 7 akun yang membalas pesan yang dikirim penulis dan hasilnya adalah:

Tabel 3. Hasil Pengetesan Pertama

Skenario	Hasil
Menawarkan pekerjaan dan mengajak bekerja	1 Nomor kontak, 1 Informasi daerah tempat tinggal, 1 akun yang memblokir, 1 akun mengabaikan pesan
Berpura-pura sebagai konsumen	1 Nomor kontak, Informasi koneksi dari target
Berpura-pura sebagai orang penting	1 Nomor kontak, 1 akun yang curiga

Pengetesan berikutnya menggunakan cara "*friendly"* yaitu dengan meminta pertemanan kepada 74 target dengan menggunakan akun yang berbeda bernama "Wulan Nurhayati". Hasilnya adalah terdapat 28 akun yang menerima permintaan pertemanan penulis, berikut adalah hasilnya:

Tabel 4. Hasil Menggunakan Metode "*Friendly*"

Skenario	Hasil
Berkenalan	- 5 nomor kontak - 5 informasi daerah - 1 Informasi pribadi
Berpura-pura sebagai konsumen	- 2 nomor kontak relasi dari target - 3 nomor kontak target - 2 informasi jabatan - 1 alamat

Hasil dari pendekatan yang dilakukan dengan menggunakan metode "*friendly*" lebih baik karena bisa mendapatkan informasi yang cukup beragam dan mendetail, namun metode ini membutuhkan waktu yang cukup lama sebab diharuskan membuat target nyaman dan tidak curiga terlebih dahulu.

3.1 Strategi Mitigasi

1. Persiapan
   a. Pelatihan kesadaran terhadap warga untuk meningkatkan kesadaran tentang *social engineering*, termasuk contoh serangan dan cara mengidentifikasinya;
   b. Segera laporkan akun yang melakukan penipuan;
   c. Selalu aktifkan fitur *two authentication factor* untuk meminimalisir ancaman pengambil alihan akun;
   d. Jika si pelaku berpura-pura menjadi seseorang yang dikenal, segera hubungi terlebih dahulu orang tersebut dan konfirmasi apakah akun ini adalah akun miliknya atau bukan, serta perjelas apakah ia mengirim pesan atau tidak;

e. Segera hubungi bank dan beritahukan bahwa akun sudah terkena kasus penipuan, dan jika ada yang berpura-pura menjadi anda untuk mengganti pin atau apapun itu, segera tolak;
f. Segera siapkan kontak pihak berwajib untuk melaporkan kejadian kartu tanda penduduk sudah tersebar.

2. Deteksi dan Analisis
   a. Segera *screenshot* semua pesan yang anda lakukan dengan si pelaku, ini adalah bentuk barang bukti;
   b. Selalu cek pengirim pesan baik itu melalui email, sms, ataupun messenger Facebook, sebab hampir semua akun perusahaan besar di Indonesia sudah memiliki logo centang biru sebagai pembeda dengan penipu;
   c. Lihat baik-baik penulisan dari pengirim pesan, jika ada satu karakter yang menurut pengguna tidak benar, maka jangan hiraukan pesan itu dan laporkan pesan tersebut;
   d. Mintalah nomor kontak si pelaku jika ia mengaku sebagai seorang HRD/pihak berwenang/kenalan, kemudian lakukan cek nomor pada aplikasi *Get Contact*;
   e. Jangan percaya pada pesan yang membuat anda merasa takut, seperti akun yang akan dihapus atau pesan dari pihak berwenang.
3. *Containment*
   a. Segera laporkan pesan dari pelaku sebagai Spam, agar pesan yang sama tidak akan bisa dilihat oleh orang lain;
   b. Jika si pelaku memberikan tautan atau *link*, segera cek link tersebut apakah masuk ke dalam daftar website berbahaya dengan cara cek (https://openphish.com/) *website* tersebut berisi daftar tautan yang berbahaya, kemudian laporkan *website phishing* ke Google dengan mengakses (https://search.google.com/search-console/report-spam?hl=id);
   c. Jika si pelaku menawarkan pekerjaan dan anda diberi sebuah formulir yang mengharuskan anda memberi kartu tanda penduduk anda, segera laporkan formulir tersebut dengan alasan penyalahgunaan;
   d. Jika si pelaku meminta alamat email, segera ubah sandi email tersebut untuk meminimalisir ancaman *takeover* akun.
4. Eradikasi
   a. Jika informasi pribadi terekspos di *internet*, segera hubungi pihak *platform* tersebut untuk menghapus informasi tersebut;
   b. Blokir akun pelaku;
   c. Ubah semua kata sandi yang menggunakan informasi pribadi, seperti tanggal lahir atau nama anggota keluarga.
5. Pemulihan
   a. Selalu pantau *website* penipuan apakah sudah di nonaktifkan pihak berwenang;
   b. Menerapkan anti-virus untuk melakukan pengecekkan berkala terhadap sistem yang anda miliki;
   c. Pastikan akun pelaku sudah tidak aktif;
   d. Ubah pin bank anda dengan langsung menghadiri pihak bank tersebut;
   e. Laporan terkait pencurian identitas ke instansi Pemerintahan agar anda bisa mendapatkan pembaruan identitas;
6. Tindak Lanjut
   a. Buat dokumentasi untuk memberikan pelajaran kepada pengguna lain;
   b. Mengambil pelajaran dari insiden ini untuk melakukan pencegahan terhadap ancaman berikutnya;
   c. Buat daftar kontak pihak berwenang, agar jika ada serangan lanjutan, pengguna bisa menghubungi pihak-pihak tersebut dengan lebih cepat.

4. Kesimpulan

Penelitian ini menganalisis ancaman social engineering terhadap pengguna Facebook di Desa Bojong Emas RW 04 menggunakan pendekatan *Open Source Intelligence* (OSINT). Hasil investigasi menunjukkan bahwa banyak pengguna Facebook di RW 04 Desa Bojong Emas memiliki kesadaran rendah terhadap ancaman social engineering dan sering menyebarkan informasi pribadi secara publik. Hal ini meningkatkan risiko pencurian identitas dan penipuan finansial. Meskipun fitur keamanan Facebook cukup efektif untuk mengurangi ancaman ini, penelitian ini menunjukkan bahwa teknik OSINT efektif dalam mengidentifikasi potensi ancaman dan kelemahan keamanan informasi pengguna. Dengan menganalisis data publik dan menerapkan taktik *social engineering*, penelitian ini berhasil mengungkap berbagai kerentanan. Berdasarkan temuan ini, beberapa rekomendasi mitigasi dikembangkan untuk meningkatkan keamanan pengguna Facebook di Desa Bojong Emas RW 04. Rekomendasi tersebut mencakup edukasi keamanan siber untuk meningkatkan kesadaran pengguna dan penerapan pengaturan privasi yang lebih ketat.

Daftar Pustaka

[1] APJII. (2023). APJII: Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang. Diakses pada 24 Maret 2024, dari https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

[2] Badan Siber dan Sandi Negara Republik Indonesia (BSSN). (2024). Laporan Bulanan Januari 2024. Jakarta: ID-SIRTII/CC.

[3] Badan Siber dan Sandi Negara Republik Indonesia (BSSN). (2024). Laporan Bulanan Februari 2024. Jakarta: ID-SIRTII/CC.

[4] Akhtar, H. (2020). Perilaku Oversharing di Media Sosial: Ancaman atau Peluang? Psikologika : Jurnal Pemikiran dan Penelitian Psikologi, 25(2), 257–270. https://doi.org/10.20885/psikologika.vol25.iss2.art7

[5] Pallivalappil, A. S., S. N., J., & K., K. P. (2021). Social Engineering Attacks on Facebook – A Case Study. International Journal of Case Studies in Business, IT, and Education, 299–313. https://doi.org/10.47992/IJCSBE.2581.6942.0135

[6] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, dan M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," IEEE Access, vol. 10, hlm. 39325–39343, 2022, doi: 10.1109/ACCESS.2022.3162594.

[7] Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques – a review of Cyber Defense Mechanisms. IJARCCE, 11(7). https://doi.org/10.17148/ijarcce.2022.11728

[8] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Nomor 39 /POJK.03/2019 tentang Penerapan Strategi Anti Fraud Bagi Bank Umum," Otoritas Jasa Keuangan, 2019, https://www.ojk.go.id/id/regulasi/Documents/Pages/Penerapan-Strategi-Anti-Fraud-Bagi-Bank-Umum/pojk%2039-2019.pdf .

[9] Badan Siber dan Sandi Negara, "Panduan Penanganan Insiden Serangan Phishing" Badan Siber dan Sandi Negara, 2018 https://cloud.bssn.go.id/s/qRbKcS3Ndr65nBk.

[10] International Master in Security, Intelligence & Strategic Studies 2019. (2019, July). Tracking the flow of military assets and logistics for OSINT: The case of the Syrian Civil War

[11] Maekel Eugaliel Pindonta Sembiring dan Arthur Josias Simon, "Papua Separatis Terrorist Groups Detection Through Osint and Counter Intelligence Effort (Osint Detection Study On The Baintelkam Polri Separatist Management Unit)," konfrontasi2, vol. 9, no. 1, hlm. 62–69, Mar 2022, doi: 10.33258/konfrontasi2.v9i1.192.

[12] P. K. Narasimhan dkk., "Open-source Intelligence (OSINT) investigation in Facebook," ei, vol. 35, no. 3, hlm. 357-1-357–12, Jan 2023, doi: 10.2352/EI.2023.35.3.MOBMU-357.

[13] F. Gunawan dan T. M. M. Keumala, "Analisis Information Gathering Target Daftar Pencarian Orang Menggunakan Metodeopen Source Intelligence Pada Kejaksaan Tinggi Aceh," vol. 4, no. 1, 2024.

[14] N. Bansla, S. Kunwar, dan Khushboo Gupta, "Social Engineering: A Technique for Managing Human Behavior," Mar 2019, doi: 10.5281/ZENODO.2580822.

[15] N. F. Amin, S. Garancang, dan K. Abunawas, "KONSEP UMUM POPULASI DAN SAMPEL DALAM PENELITIAN".