Psikosospen : Jurnal Psikososial dan Pendidikan
https://publisherqu.com/index.php/psikosospen/
Vol. 2 No. 1 Maret 2026
https://issn.brin.go.id/terbit/detail/20250326030437435

ANALISIS PERILAKU CYBER HYGIENE: STRATEGI MELINDUNGI DATA PRIBADI DARI RISIKO KEBOCORAN PINJAMAN ONLINE

Anan Dita Asrawati[1], Nur Riswandiy Marsuki[2]
Pendidikan Sosiologi, Universitas Muhammadiyah Makassar[1,2,3]
Email: ananditaasrawati@gmail.com

Abstrak

Maraknya platform pinjaman online ilegal di Indonesia membawa risiko serius terhadap keamanan data pribadi, mulai dari penambangan data yang agresif hingga teror penagihan. Meskipun risiko ini nyata, terjadi fenomena privacy paradox di mana pengguna tetap bersedia menukar privasi mereka demi akses dana cepat. Penelitian ini bertujuan untuk menganalisis perilaku cyber hygiene dan strategi perlindungan data pribadi yang dilakukan pengguna aplikasi pinjaman online dalam menghadapi risiko kebocoran data. Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus. Pengumpulan data dilakukan melalui wawancara mendalam dan observasi digital terhadap pengaturan gawai pengguna. Hasil penelitian menunjukkan bahwa secara prosedural, praktik cyber hygiene pengguna tergolong rendah, yang ditandai dengan perilaku memberikan izin akses penuh (allow all permissions) tanpa membaca kebijakan privasi akibat desakan ekonomi dan pola pikir kelangkaan (scarcity mindset). Namun, pengguna mengembangkan strategi pertahanan diri (coping strategies) yang adaptif. Strategi tersebut meliputi tindakan preventif berupa manipulasi identitas (menggunakan perangkat sekunder, memalsukan nama kontak darurat, dan merekayasa isi galeri foto) serta tindakan represif berupa pemutusan jejak digital (mengganti kartu SIM dan menonaktifkan media sosial) saat menghadapi teror penagihan. Penelitian ini menyimpulkan bahwa pengguna telah bertransformasi dari objek pasif menjadi subjek aktif yang memanfaatkan celah sistem untuk melindungi diri, meskipun metode yang digunakan cenderung manipulatif.

Kata Kunci : Cyber Hygiene, Pinjaman Online, Perlindungan Data Pribadi, Privacy Paradox, Strategi Pertahanan Diri

Abstract

The proliferation of illegal online lending platforms (pinjaman online) in Indonesia poses serious risks to personal data security, ranging from aggressive data mining to debt collection terror. Despite these evident risks, a privacy paradox phenomenon persists where users willingly trade their privacy for quick fund access. This study aims to analyze cyber hygiene behaviors and personal data protection strategies employed by online lending users in facing data breach risks. The study employs a qualitative method with a case study approach. Data were collected through in-depth interviews and digital observations of users' device settings. The results indicate that procedurally, users' cyber hygiene practices are low, characterized by granting full access permissions (allow all permissions) without reading privacy policies due to economic pressure and a scarcity mindset. However, users have developed adaptive coping strategies. These include preventive measures such as identity manipulation (using secondary devices, falsifying emergency contact names, and engineering photo gallery content) and

repressive measures such as severing digital traces (changing SIM cards and deactivating social media) when facing collection terror. The study concludes that users have transformed from passive objects into active subjects who exploit system loopholes to protect themselves, albeit through manipulative methods
Keywords : Cyber Hygiene, Online Lending, Personal Data Protection, Privacy Paradox, Coping Strategies.

PENDAHULUAN

Perkembangan teknologi finansial (fintech) di Indonesia, khususnya layanan Peer-to-Peer (P2P) Lending atau pinjaman online, telah mengubah lanskap akses keuangan masyarakat secara drastis. Fenomena ini tidak hanya didorong oleh kemudahan teknologi, tetapi juga oleh perubahan perilaku konsumtif dan kebutuhan sosial masyarakat. Studi terbaru menunjukkan bahwa pinjaman online kini dianggap sebagai kebutuhan yang tidak terelakkan bagi sebagian masyarakat, bahkan penggunaannya sering kali didorong oleh faktor psikologis Fear of Missing Out (FOMO) untuk memenuhi gaya hidup (Amos et al., 2024). Di kalangan mahasiswa, pinjaman online sering digunakan untuk mendukung status sosial melalui perilaku konsumtif, seperti membeli barang bermerek, meskipun mereka belum memiliki penghasilan tetap. Namun, tingginya permintaan ini dimanfaatkan oleh pelaku kejahatan siber melalui maraknya platform pinjaman online ilegal. Data terbaru dari Otoritas Jasa Keuangan (OJK) mencatat bahwa Satgas Pasti telah menghentikan ribuan entitas keuangan ilegal, termasuk 796 entitas pinjaman online ilegal pada periode Oktober hingga Desember 2024 saja ((OJK), n.d. 2025).

Masalah utama dalam ekosistem peminjaman online, terutama yang illegal, adalah metode pengumpulan informasi yang sangat agresif dan tidak bermoral. Studi menunjukkan bahwa penyalahgunaan informasi pribadi pengguna kerap terjadi melalui pengumpulan data tanpa izin, eksploitasi data secara tidak etis, hingga distribusi data kepada pihak ketiga tanpa persetujuan dari pemiliknya (Sari & Nasution, 2024). Aplikasi pinjaman yang tidak sah sering kali meminta izin akses yang terlalu banyak pada alat pengguna, yang kemudian disalahgunakan untuk melakukan penagihan secara ilegal dengan ancaman dan teror psikologis (Angin et al., 2025). Risiko ini semakin diperburuk oleh kekurangan dalam sistem internal di platform digital yang sering kali tidak dilengkapi dengan sistem penyimpanan data yang memadai atau perlindungan firewall yang cukup, sehingga meningkatkan kemungkinan terkena serangan siber (Pardosi et al., 2024).

Meskipun ancaman terhadap penyalahgunaan data sangat ada, terdapat fenomena yang bertentangan di mana individu masih mau memberikan informasi pribadi mereka. Ini menunjukkan adanya perbedaan antara aturan hukum yang seharusnya diterapkan dan kenyataan perilaku orang-orang, yang dikenal dengan istilah privacy paradox (Awareness et al., 2025). Meskipun Indonesia sudah meratifikasi Undang-Undang Nomor 27 Tahun 2022 mengenai Perlindungan Data Pribadi (UU PDP) sebagai landasan hukum, sejauh mana perlindungan ini dapat berjalan dengan baik sangat tergantung pada pelaksanaannya di lapangan dan tingkat kesadaran pengguna (Rifa & Hidayati, 2024). Faktanya, pemahaman pengguna mengenai pentingnya perlindungan privasi dan keamanan informasi masih tergolong rendah, menyebabkan banyak orang tidak menyadari bahwa informasi pribadi mereka merupakan sesuatu yang perlu dijaga layaknya aset keuangan. Kesenjangan ini dikenal sebagai kurangnya penerapan praktik kebersihan siber, di mana pengguna seringkali mengabaikan langkah-langkah keamanan dasar karena tertekan oleh kebutuhan ekonomi (Ardana & Kornelis, 2024). Oleh karena itu, penelitian ini akan berfokus pada analisis perilaku cyber hygiene dan strategi perlindungan data pribadi yang dilakukan pengguna aplikasi pinjaman online dalam menghadapi risiko kebocoran data.

METODE PENELITIAN

Penelitian ini menerapkan metode kualitatif dengan pendekatan studi kasus untuk menginvestigasi secara menyeluruh perilaku cyber hygiene dan strategi perlindungan data pribadi pengguna aplikasi pinjaman daring. Metode kualitatif dipilih karena penelitian ini bertujuan untuk memahami fenomena perilaku manusia dalam konteks aslinya, dengan peneliti berperan sebagai alat utama dalam mengungkap makna di balik tindakan manajemen privasi dari subjek yang diteliti (Creswell & Creswell, 2017). Melalui metode studi kasus, penelitian ini fokus pada satu unit analisis, yaitu perilaku pengguna dalam fintech lending terkait dengan risiko kebocoran data. Hal ini memungkinkan peneliti untuk mendapatkan gambaran lengkap dan mendalam mengenai fenomena privacy paradox yang terjadi di lapangan (Yin, 2023).

Pemilihan peserta penelitian (informan) dilakukan dengan cara purposive sampling, artinya informan dipilih berdasarkan pertimbangan dan kriteria tertentu yang relevan dengan tujuan penelitian, bukan secara acak (Sugiyono, 2022). Kriteria yang ditentukan untuk informan dalam studi ini adalah orang yang aktif menggunakan atau pernah menggunakan

aplikasi pinjaman online (baik yang legal maupun ilegal) dalam satu tahun terakhir serta memiliki pengalaman terkait isu keamanan data atau ancaman privasi. Data dikumpulkan melalui dua metode utama, yaitu wawancara mendalam untuk menggali aspek motivasi dan pemahaman kognitif pengguna, serta observasi digital terhadap perangkat yang digunakan informan untuk melihat praktik langsung tentang pengaturan izin aplikasi dan fitur keamanan yang diterapkan.

Analisis data dilakukan menggunakan model interaktif yang dikembangkan oleh (Miles et al., 2014) melalui tiga tahap yang berlangsung secara bersamaan, yaitu pengurangan data, penyajian data, dan penarikan kesimpulan. Proses ini dimulai dengan memilah data dari wawancara dan observasi yang relevan dengan indikator cyber hygiene, lalu menyajikannya dalam bentuk narasi deskriptif untuk menemukan pola pertahanan diri pengguna. Untuk memastikan kevalidan temuan, peneliti menerapkan teknik triangulasi sumber dengan membandingkan konsistensi antara pernyataan informan saat wawancara dan bukti perilaku yang ditemukan selama observasi pada perangkat digital mereka.

HASIL PENELITIAN

Perilaku "Klik Tanpa Baca" dan Pengabaian Izin Akses

Hasil pengamatan pada perangkat yang digunakan oleh informan mengindikasikan bahwa hampir semua subjek penelitian tidak memeriksa Syarat dan Ketentuan saat mengunduh aplikasi. Informan cenderung menekan tombol "Izinkan" secara otomatis untuk setiap permohonan akses sistem, termasuk izin untuk mengakses kontak, riwayat panggilan, dan foto di galeri. Saat dikonfirmasi melalui wawancara, informan mengatakan bahwa tindakan ini didorong oleh anggapan bahwa membaca kebijakan privasi hanya akan memperlambat proses pencairan dana, sementara kebutuhan mereka sangat mendesak.

Kondisi ini semakin buruk karena tampilan aplikasi sering menggunakan pola yang merugikan, dengan tombol persetujuan yang sangat menonjol sementara tautan kebijakan privasi dibuat kecil atau sulit ditemukan, sehingga secara psikologis memaksa pengguna untuk tidak membaca. Selain itu, beberapa narasumber menyatakan merasa 'terjebak' karena aplikasi tidak akan beroperasi sama sekali jika satu izin akses ditolak, yang menghilangkan kesempatan bagi pengguna untuk melakukan negosiasi terkait privasi.

Manipulasi Identitas sebagai Strategi Pertahanan Awal

Temuan menarik lainnya adalah adanya usaha untuk memanipulasi data yang dilakukan oleh peminjam yang sering bertransaksi. Beberapa responden mengaku dengan sengaja menggunakan "Nomor Sekunder" yang tidak terhubung dengan anggota keluarga utama ketika mendaftar untuk aplikasi pinjaman online yang ilegal. Di samping itu, juga ditemukan praktik pemalsuan nama kontak di daftar telepon mereka; contohnya, menyebut nomor teman kerja dengan nama "Paman" atau "Bibi" untuk memenuhi syarat keberadaan kontak darurat keluarga, serta untuk menipu sistem penagihan agar tidak mengganggu keluarga asli mereka jika terjadi masalah pembayaran.

Strategi pengaruh ini tidak hanya terfokus pada interaksi langsung, tetapi juga mencakup pengaturan galeri foto; beberapa narasumber dengan sengaja mengisi galeri mereka dengan gambar-gambar umum atau lanskap yang diambil dari internet, menggantikan foto wajah mereka sendiri, untuk mengurangi kemungkinan penyalahgunaan foto untuk intimidasi seksual atau pencemaran nama baik (doxing) yang sering dilakukan oleh oknum penagih.

Respons Reaktif: Pemutusan Akses Digital

Saat berada dalam tahap penagihan yang disertai intimidasi, sikap cyber hygiene informan beralih menjadi sangat defensif. Langkah yang paling sering diambil adalah menghapus aplikasi, mengganti kartu SIM, dan menonaktifkan akun media sosial (Instagram/Facebook) guna menghindari jejak digital yang bisa dilacak oleh penagih utang. Peralihan perilaku dari yang awalnya pasif menjadi sangat defensif sering kali dipicu oleh peningkatan teror yang mulai menyentuh aspek sosial individu, seperti ketika penagih mulai menghubungi atasan di tempat kerja atau membentuk grup WhatsApp yang berisi anggota keluarga korban. Dalam keadaan panik ini, pemikiran rasional tentang kerugian dari mengganti nomor (hilangnya hubungan lama) menjadi tidak penting dibandingkan dengan kebutuhan mendesak untuk memperoleh ketenangan pikiran. Informan melihat langkah-langkah isolasi digital ini sebagai satu-satunya metode yang ampuh untuk menghentikan tekanan psikologis.

Agar dapat memetakan pola perilaku tersebut secara lebih sistematis, mulai dari aspek rendahnya kepatuhan prosedur hingga ragam strategi pertahanan diri yang diterapkan pengguna, ringkasan temuan penelitian disajikan dalam Tabel berikut ini.

Kategori Perilaku	Bentuk Tindakan Nyata (Observed Action)	Deskripsi Temuan Lapangan	Motivasi/Alasan Penggunaan (Hasil wawancara)
Kepatuhan Prosedur *(Security Compliance)*	Pengabaian Izin Akses	Pengguna langsung menyetujui (*Allow All*) permintaan akses kontak, galeri, dan lokasi tanpa seleksi.	Prioritas kecepatan pencairan dana; persepsi bahwa membaca syarat ketentuan membuang waktu.
	Buta kebijakan Privasi	Pengguna melewatkan (skip) halaman Terms & Conditions dalam hitungan detik.	Bahasa hukum sulit dipahami; merasa tidak punya pilihan lain jika ingin pinjaman disetujui.
Strategi Preventif *(Sebelum Meminjam)*	Manipulasi Identitas	Menggunakan nama samaran pada kontak di buku telepon (misal: teman dinamai 'Ayah') untuk mengecoh sistem verifikasi.	Melindungi kerabat asli dari potensi teror penagihan (*debt collector*).
	Isolasi Perangkat	Menggunakan gawai sekunder ("HP Kosongan") atau menghapus data sensitif di galeri sebelum instalasi.	Membatasi jumlah data pribadi yang bisa diambil (harvesting) oleh aplikasi.
Strategi Represif *(Saat Penagihan)*	Pemutusan Jejak Digital	Mengganti kartu SIM, memblokir nomor tidak dikenal, hingga menonaktifkan akun	Menghindari tekanan psikologis dan intimidasi yang dilakukan penagih secara masif.

		media sosial.	
	Penghapusan Aplikasi	Melakukan uninstall aplikasi segera setelah dana cair atau saat jatuh tempo	Memutus akses pelacakan lokasi (real-time location) oleh pihak aplikasi.

Pembahasan

Analisis Kesenjangan Literasi dan Kepatuhan Keamanan Data

Temuan dari penelitian ini menegaskan adanya situasi di mana literasi digital tidak sejalan dengan tindakan keamanan. Pengguna menyadari adanya risiko, tetapi tetap melanggar prosedur keamanan. Hal ini sesuai dengan penelitian (Meladiah, 2024) yang mengungkapkan bahwa perlindungan hukum terhadap data pribadi sering kali tidak efektif, bukan karena kurangnya aturan, tetapi karena fenomena masyarakat yang dengan sukarela mengorbankan hak privasi demi mendapatkan akses ekonomi yang lebih mudah. Dalam hal ini, pengguna melihat data pribadi sebagai "mata uang" yang dapat ditukar, suatu perilaku yang membuat mereka rentan terhadap eksploitasi oleh platform ilegal yang tidak memiliki standar keamanan enkripsi yang cukup baik.

Fenomena ini juga dapat dijelaskan dengan sudut pandang pola pikir kelangkaan, di mana tantangan ekonomi menimbulkan semacam 'penglihatan terowongan' pada individu, sehingga perhatian mereka hanya terpusat pada solusi jangka pendek, yaitu pencairan dana dan mengabaikan potensi risiko keamanan yang dapat muncul dalam jangka panjang.

Dinamika Psikologis dan Strategi *Coping* Pengguna

Strategi dalam manipulasi data dan isolasi digital yang ditemukan dalam penelitian ini berfungsi sebagai mekanisme perlindungan diri terhadap tekanan mental. (Rezky & Sulaiman, 2024) dalam kajiannya menekankan bahwa penggunaan layanan pinjaman fintech menimbulkan risiko psikologis yang signifikan, termasuk kecemasan dan stres akibat metode penagihan yang agresif. Temuan mengenai penggunaan data palsu menunjukkan bahwa pengguna sebenarnya memiliki kemampuan teknis untuk beradaptasi dan melawan algoritma aplikasi, namun kemampuan tersebut digunakan untuk tujuan manipulatif alih-alih untuk perlindungan yang sebenarnya.

Tindakan 'memanipulasi' sistem aplikasi pinjaman online ini mencerminkan adanya perubahan perilaku pengguna. User yang sebelumnya hanya menjadi sasaran pasif dalam

eksploitasi data, saat ini mulai berubah menjadi pihak yang aktif dengan berusaha membalikkan situasi dengan memanfaatkan kelemahan dalam proses verifikasi sistem fintech itu.

Urgensi Pengawasan Pihak Ketiga dalam Ekosistem Pinjol

Tindakan pengguna yang memutuskan untuk mengubah nomor atau menghapus akun mereka menunjukkan adanya kelemahan dalam sistem perlindungan konsumen di bidang penagihan. (Ratuwalu & Dewayani, 2026) menegaskan bahwa meskipun OJK telah menerbitkan peraturan baru mengenai perlindungan konsumen (POJK No. 22 Tahun 2023), praktik penagihan yang dilakukan oleh pihak ketiga (debt collector) masih sering melanggar privasi, sehingga memaksa konsumen untuk mengambil tindakan defensif yang ekstrem. Mekanisme pemeriksaan dan keseimbangan dalam ekosistem pinjaman digital masih kurang seimbang karena saat ini fokus pada aspek keamanan terlalu tergantung pada kewaspadaan masing-masing pengguna (keamanan yang berorientasi pada pengguna), sedangkan seharusnya penyedia platform harus memiliki tanggung jawab yang lebih besar dalam memastikan keamanan struktur data mereka. Selain itu, (Rustam & IBLAM, 2025)menyoroti bahwa platform fintech yang mengelola data seharusnya bertanggung jawab sepenuhnya atas keamanan informasi nasabah. Namun, kelalaian pengguna dalam memberikan izin akses sering dimanfaatkan oleh platform sebagai alasan untuk menghindari tanggung jawab ketika terjadi kebocoran data.

KESIMPULAN

Penelitian ini menemukan bahwa penerapan cyber hygiene di kalangan pengguna aplikasi pinjaman online masih berada pada tingkat yang rendah, yang terlihat dari tingginya perilaku "klik tanpa membaca" dan pengabaian izin akses yang berlebihan. Rendahnya kepatuhan terhadap prosedur keamanan ini tidak hanya disebabkan oleh kurangnya pemahaman teknis, tetapi juga dipengaruhi oleh tekanan ekonomi dan pola pikir kelangkaan yang mendorong pengguna untuk lebih mengutamakan kecepatan dalam mendapatkan dana daripada melindungi data pribadi mereka.

Meskipun kepatuhan proseduralnya rendah, pengguna menunjukkan kemampuan adaptasi dengan mengembangkan dua bentuk strategi pertahanan diri (coping strategies) untuk memitigasi risiko. Pertama, strategi preventif yang bersifat manipulatif, di mana pengguna melakukan rekayasa identitas sebelum meminjam, seperti menggunakan perangkat

sekunder ("HP kosongan"), memalsukan nama kontak darurat, hingga mengisi galeri dengan foto palsu untuk mengecoh sistem verifikasi. Kedua, strategi represif yang bersifat reaktif saat terjadi penagihan, yaitu dengan melakukan pemutusan jejak digital secara total melalui penggantian kartu SIM, penghapusan aplikasi, dan penonaktifan akun media sosial.

Secara keseluruhan, temuan ini mengindikasikan adanya pergeseran perilaku pengguna dari objek pasif menjadi subjek aktif yang berusaha membalikkan keadaan dengan memanfaatkan celah sistem fintech. Namun, penelitian ini juga menegaskan bahwa mekanisme perlindungan saat ini masih timpang karena terlalu membebankan keamanan pada kewaspadaan pengguna (user-centric), sehingga diperlukan tanggung jawab yang lebih besar dari penyedia platform untuk membenahi arsitektur keamanan data mereka

DAFTAR PUSTAKA

(OJK), O. J. K. (n.d.). Siaran Pers: Satgas PASTI Blokir 796 Entitas Ilegal di Oktober s.d. Desember 2024. *Siaran Pers Otoritas Jasa Keuangan. Jakarta: OJK*. https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Satgas-Pasti-Blokir-796-Entitas-Ilegal-di-Oktober---Desember-2024.aspx

Amos, V., Papalangi, N., Atma, U., & Makassar, J. (2024). PINJAMAN ONLINE : PERILAKU MASYARAKAT DALAM MENGHADAPI FEAR OF MISSING OUT (FOMO). *Jurnal Manajemen Dan Bisnis Jayakarta, 6(1)*, *6*(1), 83–94.

Angin, D. P., Sunarmi, Sukarja, D., & Harianto, D. (2025). *Perlindungan Hukum Nasabah Pinjaman Online Ilegal dalam Hal Penagihan secara Melawan Hukum dengan Menyalahgunakan Data Pribadi*. *4*(4), 238–253.

Ardana, S. T., & Kornelis, Y. (2024). Penyalahgunaan data pribadi pada pinjaman online di Indonesia: Analisis perlindungan dan sanksi hukum. *Legalite: Jurnal Perundang Undangan Dan Hukum Pidana Islam*, *9*(1), 1–11.

Awareness, P., Darnela, L., Rusdiana, E., Islam, U., Sunan, N., Yogyakarta, K., & Madura, U. T. (2025). *Supremasi Hukum : Jurnal Kajian Ilmu Hukum*. *14*(1), 1–28. https://doi.org/10.14421/2gg2rp29

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Meladiah, R. (2024). *Perlindungan Hukum Terhadap Data Pribadi Pengguna Aplikasi Pinjaman Online*. *3*(6), 5895–5904.

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). Qualitative data analysis: A methods sourcebook. *(No Title)*.

Pardosi, V. B. A., Deta, B., Nugroho, F., & Vandika, A. Y. (2024). *SISTEM KEAMANAN INFORMASI*. http://repository.undha.ac.id/1645/1/Sistem Keamanan Informasi.pdf

Ratuwalu, R., & Dewayani, S. (2026). *Perlindungan Hukum Konsumen Fintech P2P Lending akibat Penagihan oleh Pihak Ketiga sesuai POJK No . 22 Perlindungan Konsumen*

melakukan penagihan kepada konsumen yang menunggak pembayaran . Sayangnya , praktik. *5*(September 2025).

Rezky, D., & Sulaiman, A. (2024). *Studi Literatur : Risiko Psikologis Penggunaan Fintech Lending pada Mahasiswa*. *7*(2), 197–201.

Rifa, F., & Hidayati, M. N. (2024). Kebijakan Penal dalam Perlindungan Data Pribadi Nasabah Fintech Lending di Indonesia. *Binamulia Hukum*, *13*(2), 461–481.

Rustam, M. R., & IBLAM, S. (2025). *Tanggung Jawab Hukum Platform Fintech Per to Peer Lending terhadap Penyalahgunaan Data Pribadi Nasabah Berdasarkan UU No . 27 Tahun 2022 Tentang Perlindungan Data Pribadi*. *May*.

Sari, suci indah, & Nasution, M. I. P. (2024). Penyalahgunaan Data Pribadi Konsumen Terhadap Pinjaman Online Ilegal. *Jurnal Hukum Dan Kewarganegaraan*. https://doi.org/10.3783/causa.v4i8.3740

Sugiyono, P. D. (2022). *DAN R & D*.

Yin, R. K. (2023). *research question than a*. *11*(1), 2016–2019.

Email

pendidikansosiologi@unismuh.ac.id