ANALISIS RISIKO KEAMANAN PRIVASI PENGGUNA PADA PENGGUNAAN FITUR SIMPAN SANDI OTOMATIS DI BROWSER

LAILATUL FITALIQOH

Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia, 5026231229@Student.Its.Ac.Id

NUR AINI RAKHMAWATI

Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia, Nur.Aini@Its.Ac.Id

ABSTRACT

Penggunaan fitur penyimpanan sandI otomatis di browser web memberikan kemudahan yang signakan bagi pengguna dengan menyederhanakan proses login di berbagai akun digital terutama untuk sandi yang rumit Meskipun begitu fitur ini juga menimbulkan sejumlah kekhawatiran terhadap keamanan dan privasi termasuk potensi kebocoran data serangan phishing dan akses tanpa izin Penelitian ini bertujuan untuk menganalisis polapola penggunaan persepsi manfaat serta tingkat kesadaran risiko pengguna terhadap fitur ini Metode penelitian menggunakan pendekatan campuran yaitu surveikuantitatif dan kualitatifserta tinjauan literatur akademik terkait untuk memperkuat analisis.

Hasil penelitian menunjukkan bahwa setengah dari peserta sering menggunakan fitur tersebut karena kemudahannya sementara hampir 40 persen jarang menggunakannya karena kekhawatiran tentang keamanan dan sekitar 11 persen sama sekali tidak menggunakan fiturnya dengan alasan yang serupa. Sebagian besar peserta (sekitar 78 persen) mengakui manfaat dari penggunaan fitur ini dalam membantu mengelola kata sandinya namun sekitar 69 persen juga menyadari risiko yang terlibat seperti pencurian perangkat,pishing,dan lupa logout.Beberapa peserta melaporkan pengalaman mereka dalam menghadapi ancaman keamanan,tetapi tidak semua dari mereka melakukan langkah-langkah perlindungan yang memadai.

Studi ini menyoroti karakteristik dual dari fitur penyimpanan sandinya otomatis yang melibatkan manfaat yang penting dan risiko yang terdapat di dalamnya. Oleh karena itu adalah signifikansi untuk meningkatkan keamanan dari fungsionalitas tersebut dengan memberikan edukasi kepada pengguna serta mempromosikan tindakan pencegahan seperti penggunaan autentikasi dua faktor dan pembaruan kata sandinya secara berkala sambil menghindari menyimpan kata sandinya pada perangkat publik atau bersama-sama.

Kata Kunci: Simpan Sandi, Keamanan Data, Privasi, Autentikasi Dua Faktor, Risiko

1. PENDAHULUAN

Dalam era digital saat ini, penggunaan internet telah menjadi bagian tak terpisahkan dari aktivitas sehari-hari. Berbagai platform dan layanan daring mengharuskan pengguna untuk membuat akun dengan kredensial yang unik, seperti nama pengguna dan kata sandi. Akibatnya, pengguna sering kali menghadapi tantangan dalam mengelola banyak kata sandi yang aman namun mudah diingat. Untuk mengatasi hal ini, browser modern menyediakan fitur simpan sandi otomatis (password manager) yang memungkinkan pengguna menyimpan dan mengisi kata sandi secara otomatis (Microsoft, 2022).

Meskipun fitur ini menawarkan kenyamanan dan efisiensi, penggunaannya juga memunculkan risiko terhadap keamanan dan privasi pengguna. Potensi ancaman seperti akses tidak sah, pencurian data, dan eksploitasi celah keamanan pada browser menjadi isu yang harus diperhatikan (Sharma & Kumar, 2020). Selain itu, kurangnya pemahaman pengguna terhadap mekanisme kerja fitur ini sering kali memperbesar risiko kebocoran informasi pribadi (Johnson et al., 2021).

Penelitian ini bertujuan untuk menganalisis risiko keamanan dan privasi yang dihadapi pengguna dalam penggunaan fitur simpan sandi otomatis di browser. Dengan memahami potensi ancaman dan mengevaluasi langkah mitigasi yang dapat dilakukan, penelitian ini diharapkan dapat memberikan wawasan yang bermanfaat bagi pengguna dan pengembang browser dalam meningkatkan keamanan digital.

2. METODE PENELITIAN

Untuk mendukung tujuan penelitian ini, metode penelitian yang digunakan menggabungkan pendekatan kualitatif dan kuantitatif. Penelitian ini dilakukan melalui survei langsung terhadap pengguna browser, serta analisis data yang bersumber dari jurnal dan makalah akademik terkait. Pendekatan ini bertujuan untuk mendapatkan pemahaman yang komprehensif mengenai risiko keamanan dan privasi dalam penggunaan fitur simpan sandi otomatis pada browser.

2.1 Pendekatan Penelitian

Pendekatan penelitian yang digunakan bersifat kualitatif dan kuantitatif, yang diuraikan sebagai berikut:

- Pendekatan Kualitatif

  Pendekatan ini digunakan untuk mengeksplorasi pandangan dan pemahaman pengguna terkait risiko keamanan fitur simpan sandi otomatis. Sementara analisis literatur dari jurnal dan makalah ilmiah digunakan untuk memahami kerangka teori dan konteks penelitian.

- Pendekatan Kuantitatif

  Pendekatan kuantitatif dilakukan dengan survei menggunakan kuesioner yang dirancang untuk mengukur tingkat kesadaran dan pola penggunaan fitur simpan sandi otomatis. Data kuantitatif dianalisis secara statistik untuk mengidentifikasi tren dan korelasi antara faktor-faktor risiko yang ada.

2.2 Instrumen Penelitian

Penelitian ini menggunakan beberapa instrumen sebagai berikut:

- Kuesioner Survei

  Kuesioner dirancang dengan pertanyaan tertutup dan terbuka untuk mengumpulkan data mengenai frekuensi penggunaan fitur simpan sandi otomatis, tingkat kesadaran pengguna terhadap risiko keamanan dan privasi, serta tindakan pengamanan tambahan yang dilakukan oleh pengguna.

- Studi Literatur

  Literatur yang relevan dijadikan sebagai acuan penelitian, seperti jurnal ilmiah, makalah konferensi, dan laporan keamanan, dianalisis untuk memperkuat temuan penelitian ini.

2.3 Subjek Penelitian

Populasi penelitian ini adalah pengguna browser yang menggunakan fitur simpan sandi otomatis. Sampel dipilih secara acak dengan mempertimbangkan variasi demografis seperti usia, tingkat pendidikan, dan latar belakang teknis.

3. TAHAPAN PENELITIAN

3.1 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan diantaranya menggunakan:

a. Survei disebarkan melalui platform daring yaitu Google Forms dan media sosial berupa *WhatsApp* dan Instagram untuk menjangkau responden yang lebih luas. Populasi target adalah pengguna aktif browser dengan fitur simpan sandi otomatis.

b. Analisis Dokumentasi dengan mengkaji dokumen akademik dan laporan teknis yang relevan dengan topik penelitian. Sumber utama meliputi jurnal internasional maupun nasional, laporan keamanan siber, dan makalah teknis.

3.2 Proses Tahapan

Penelitian ini dilaksanakan dalam beberapa tahapan berikut:

1. Pengumpulan literatur dengan mengumpulkan referensi dari jurnal dan makalah terkait untuk membangun landasan teori.
2. Desain kuesioner dengan menyusun pertanyaan berdasarkan tujuan penelitian.
3. Pelaksanaan survei dengan penyebaran survey dan pengisian oleh responden.
4. Analisis data dengan mengolah dan menganalisis data yang diperoleh dari survei dan studi literatur.
5. Penyusunan laporan dengan mengintegrasikan hasil analisis dalam laporan penelitian.

4. KAJIAN TEORI

Kajian teori ini bertujuan untuk memberikan landasan ilmiah terkait risiko keamanan dan privasi dalam penggunaan fitur simpan sandi otomatis di browser. Pembahasan meliputi konsep keamanan informasi, privasi digital, pengelolaan kata sandi, serta potensi ancaman yang mungkin terjadi.

4.1 Keamanan Informasi

Keamanan informasi menjadi elemen penting dalam melindungi data sensitif dari berbagai ancaman yang dapat membahayakan kerahasiaan, keutuhan, dan ketersediaan data (ISO/IEC 27001, 2013). Dalam konteks fitur simpan sandi otomatis, keamanan data yang disimpan di browser sangat bergantung pada mekanisme enkripsi yang digunakan. Jika mekanisme ini lemah, data sandi dapat menjadi target serangan oleh pihak yang tidak berwenang. Ancaman seperti pencurian data dan eksploitasi perangkat lunak sering kali menjadi fokus dalam isu keamanan informasi.

4.2 Privasi Digital

Privasi digital merujuk pada kemampuan individu untuk menjaga informasi pribadi mereka tetap aman di dunia daring (Westin, 1967). Dalam fitur simpan sandi otomatis, informasi seperti nama pengguna dan kata sandi disimpan dalam sistem yang berisiko jika tidak dikelola dengan baik. Potensi pelanggaran privasi muncul ketika data ini diakses tanpa izin, baik oleh peretas maupun oleh aplikasi pihak ketiga. Studi sebelumnya menyoroti bahwa minimnya transparansi dalam pengelolaan data pada beberapa browser dapat meningkatkan risiko privasi pengguna (Sharma & Kumar, 2020).

4.3 Pengelolaan Kata Sandi

Pengelolaan kata sandi yang efektif memainkan peran penting dalam menjaga keamanan akun daring. Fitur simpan sandi otomatis di browser dirancang untuk membantu pengguna menyimpan dan mengisi kata sandi secara praktis. Namun, kelemahan teknis seperti penyimpanan sandi yang tidak terenkripsi dengan baik atau fitur autofill yang rentan terhadap serangan phishing dapat meningkatkan risiko bagi pengguna (Bonneau et al., 2012). Penggunaan kata sandi yang kuat, unik, dan pemanfaatan pengamanan tambahan seperti kata sandi utama menjadi solusi yang disarankan untuk memitigasi risiko ini.

4.4 Model Ancaman pada Fitur Simpan Sandi Otomatis

Ancaman terhadap fitur simpan sandi otomatis dapat dikategorikan ke dalam beberapa jenis:

- Serangan Lokal

  Terjadi ketika perangkat fisik pengguna diakses oleh pihak yang tidak berwenang, misalnya melalui pencurian perangkat atau malware lokal.

- Serangan Jarak Jauh

  Memanfaatkan kerentanan pada browser atau fitur simpan sandi untuk mencuri data sandi secara daring.

- Kelalaian Pengguna

  Termasuk penggunaan sandi yang lemah, berbagi perangkat tanpa perlindungan tambahan, atau kurangnya pemahaman terhadap risiko keamanan (Johnson et al., 2021).

4.5 Studi Terkait

Penelitian sebelumnya menunjukkan bahwa pengguna cenderung memilih fitur simpan sandi otomatis karena kenyamanannya, namun sering kali mengabaikan risiko yang menyertainya. Sharma & Kumar (2020) mengidentifikasi bahwa browser populer menjadi target utama serangan karena volume data sensitif yang mereka kelola. Bonneau et al. (2012) menyoroti pentingnya edukasi pengguna tentang praktik keamanan digital, seperti penggunaan sandi yang kuat dan langkah pengamanan tambahan.

5. HASIL DAN PEMBAHASAN

5.1 Daftar Pertanyaan pada Survei

1. Seberapa sering Anda menggunakan fitur simpan sandi otomatis pada browser?

   a. Sering b. Jarang c. Tidak pernah

2. Apa alasan utama Anda menggunakan atau tidak menggunakan fitur simpan sandi otomatis? (jawaban terbuka)

3. Apakah menurut Anda fitur simpan sandi otomatis bermanfaat?

   a. Ya, sangat membantu b. Mungkin bermanfaat c. Tidak membantu

4. Apakah Anda menyadari risiko yang mungkin muncul dari penggunaan fitur ini?

a. Ya, saya sadar b. Mungkin sadar c. Tidak sadar sama sekali

5. Pernahkah Anda menghadapi risiko keamanan terkait fitur ini (misalnya pencurian perangkat, phishing, dll.)?

   a. Ya b. Mungkin pernah c. Tidak pernah

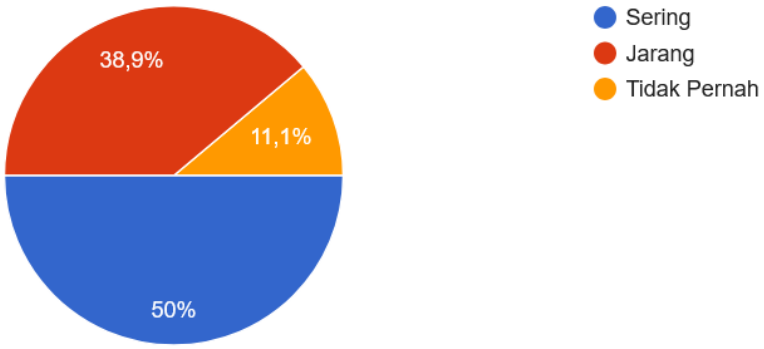
6. Jika pernah menghadapi risiko, apa langkah yang Anda ambil untuk mengatasinya? (Jawaban terbuka)

5.2 Hasil Kuesioner

5.2.1 Pola Penggunaan Fitur Simpan Sandi Otomatis pada Perangkat

Hasil survei menunjukkan variasi dalam pola penggunaan fitur simpan sandi otomatis. Dari total responden, sebanyak **38,9%** sering menggunakan fitur ini karena kemudahan login yang ditawarkannya. Sementara itu, **50%** responden jarang menggunakan fitur ini, dengan alasan utama kekhawatiran terhadap keamanan. Sebanyak **11,1%** responden bahkan tidak pernah menggunakan fitur ini, lebih memilih metode manual demi menjaga keamanan data mereka.

Hasil ini mengindikasikan bahwa fitur ini cukup populer di kalangan pengguna, tetapi ada sebagian besar yang masih mempertimbangkan risiko sebelum memanfaatkannya.

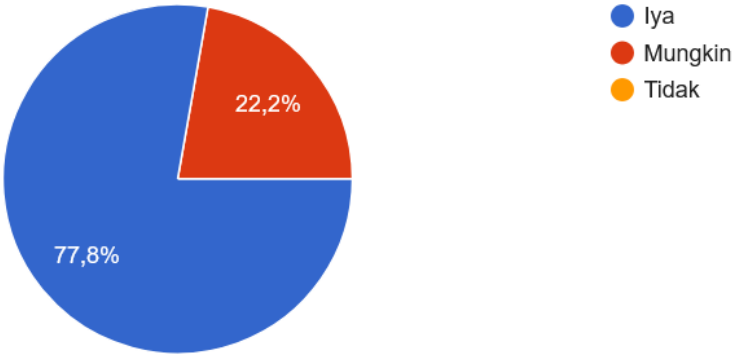


Gambar 1. Diagram Pola Penggunaan Fitur Simpan Sandi Otomatis

5.2.2 Persepsi Terhadap Manfaat Fitur Simpan Sandi Otomatis

Mayoritas responden (**77,8%**) menganggap fitur ini sangat membantu, khususnya dalam mengelola banyak akun dengan sandi kompleks. Sebanyak **22,2%** menyatakan fitur ini mungkin bermanfaat, sedangkan tidak ada responden yang menganggap fitur ini tidak berguna.

Hal ini menunjukkan bahwa manfaat fitur simpan sandi otomatis diakui oleh mayoritas pengguna, meskipun sebagian kecil masih meragukan kegunaannya.

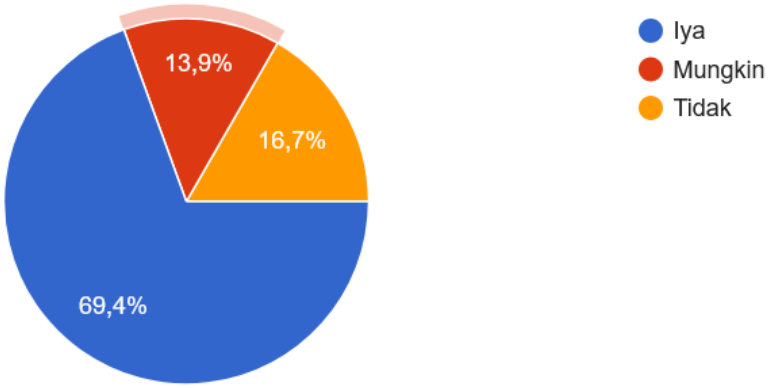


Gambar 2. Diagram Persepsi terhadap Manfaat Fitur

5.2.3 Tingkat Kesadaran Responden terhadap Risiko Penggunaan Fitur

Sebagian besar responden (**69,4%**) menyadari risiko keamanan, seperti potensi pencurian sandi atau kebocoran data. Sebanyak **13,9%** mengaku hanya sedikit menyadari risiko ini, sementara **16,7%** tidak menyadari adanya risiko sama sekali.

Temuan ini menunjukkan adanya kesadaran yang cukup baik di kalangan pengguna, tetapi juga menggarisbawahi pentingnya edukasi lebih lanjut mengenai keamanan digital dan perlindungan informasi pribadi.

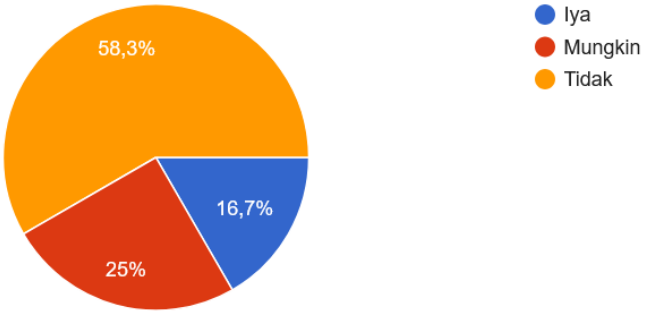


Gambar 3. Kesadaran Risiko Penggunaan Fitur

5.2.4 Pengalaman Menghadapi Risiko Keamanan

Sebanyak **16,7%** responden pernah menghadapi risiko keamanan, seperti pencurian perangkat, phishing, atau lupa logout. Sebanyak **25%** merasa mungkin pernah menghadapi risiko, sedangkan **56,3%** menyatakan tidak pernah mengalami masalah keamanan. Pengalaman yang dilaporkan meliputi:

- Pencurian perangkat: Risiko kehilangan sandi yang tersimpan.
- Peringatan login mencurigakan: Upaya login dari perangkat asing.
- Lupa logout: Akun dibiarkan terbuka di perangkat umum.
- Phishing: Kebocoran data akibat serangan phishing.
- Kerugian finansial: Akibat kebocoran data terkait akun perbankan.



Gambar 4. Pengalaman Risiko Keamanan Fitur

5.2.5 Tindakan Menghadapi Risiko Keamanan

Responden melaporkan beberapa langkah mitigasi risiko yang telah diambil, di antaranya:

- Mengganti sandi secara berkala.
- Menggunakan autentikasi dua faktor (2FA).
- Menghindari penyimpanan sandi di perangkat umum atau bersama.

Namun, sebagian responden belum melakukan langkah mitigasi spesifik setelah mengalami risiko, menunjukkan pentingnya edukasi lebih lanjut mengenai praktik keamanan digital.

5.3 Pembahasan

Fitur simpan sandi otomatis pada browser web memberikan kemudahan signifikan bagi pengguna dengan menyederhanakan proses login pada berbagai akun digital, terutama untuk sandi yang kompleks (Armaidianti, Lastono, Putra, Ghozi, & Rakhmawati, 2024). Namun, di balik kemudahannya, fitur ini menimbulkan sejumlah kekhawatiran terkait keamanan dan privasi, termasuk potensi kebocoran data, serangan *phishing*, dan akses tidak sah (Bonneau, Herley, Van Oorschot, & Stajano, 2012).

Berdasarkan hasil survei, pola penggunaan fitur simpan sandi otomatis menunjukkan perbedaan sikap pengguna, di mana faktor kenyamanan dan keamanan menjadi pertimbangan utama. Pengguna yang memanfaatkan fitur ini cenderung menghargai efisiensi yang ditawarkan, terutama untuk akun dengan sandi kompleks. Namun, kekhawatiran terhadap keamanan menjadi alasan utama bagi mereka yang jarang atau tidak menggunakan fitur ini.

Kesadaran terhadap risiko penggunaan fitur cukup tinggi di kalangan responden. Meski demikian, masih ada pengguna yang kurang memahami implikasi risiko tersebut. Temuan ini selaras dengan penelitian Sharma & Kumar (2020), yang menyatakan bahwa kurangnya edukasi pengguna meningkatkan kerentanan terhadap ancaman keamanan.

Pengalaman pengguna yang menghadapi risiko keamanan seperti pencurian perangkat atau phishing menggarisbawahi pentingnya langkah proaktif dalam melindungi data sandi. Menggunakan 2FA dan mengganti sandi secara berkala adalah langkah yang efektif, tetapi perlu dipromosikan lebih luas untuk meningkatkan kesadaran pengguna secara keseluruhan.

6. KESIMPULAN

Hasil penelitian ini menunjukkan bahwa penggunaan fitur simpan sandi otomatis pada browser memiliki keunggulan utama dalam hal kemudahan dan efisiensi, terutama bagi pengguna yang mengelola banyak akun dengan sandi kompleks. Mayoritas responden mengakui manfaat fitur ini dalam kehidupan digital sehari-hari. Namun, terdapat variasi pola penggunaan yang mencerminkan adanya kekhawatiran terhadap risiko keamanan, dengan hampir separuh responden memilih jarang atau tidak menggunakannya karena alasan privasi dan perlindungan data.

Kesadaran terhadap risiko, seperti pencurian sandi, phishing, atau lupa logout, cukup tinggi di kalangan responden. Namun, sebagian pengguna masih membutuhkan edukasi tambahan untuk memahami risiko secara lebih mendalam dan mengambil tindakan mitigasi yang tepat. Langkah-langkah seperti mengganti sandi secara berkala, menggunakan autentikasi dua faktor (2FA), dan menghindari penyimpanan sandi di perangkat publik dapat secara signifikan mengurangi risiko keamanan.

Dengan demikian, fitur simpan sandi otomatis tetap menjadi alat yang bermanfaat, tetapi penggunaannya memerlukan perhatian khusus terhadap aspek keamanan. Penting bagi pengembang browser untuk terus meningkatkan keamanan fitur ini dan bagi pengguna untuk memahami serta menerapkan praktik terbaik dalam melindungi informasi pribadi mereka. Edukasi digital yang lebih luas dapat membantu meningkatkan kesadaran dan perlindungan pengguna terhadap potensi ancaman.

ACKNOWLEDGMENT

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan dalam penyelesaian penelitian ini. Khususnya, penulis mengucapkan terima kasih kepada teknologi kecerdasan buatan (AI) yang telah memberikan kontribusi signifikan dalam proses penelitian ini. Sistem AI, terutama GPT, telah membantu dalam proses analisis data dan pembuatan konten, sedangkan Deepl telah membantu dalam menerjemahkan temuan dan konten penelitian ke dalam bahasa yang lebih jelas dan mudah dipahami.

Peran teknologi ini sangat berharga dan diakui sebagai bagian penting dalam menyelesaikan penelitian ini. Secara keseluruhan, penulis memperkirakan bahwa AI berperan sekitar 30% dalam mendukung kelancaran proses analisis dan penulisan, dengan GPT membantu menganalisis data dan Deepl mendukung dalam aspek penerjemahan.

Penulis juga mengucapkan terima kasih kepada semua responden yang telah berpartisipasi dalam survei, serta memberikan wawasan yang sangat berharga. Semoga hasil penelitian ini dapat memberikan kontribusi positif bagi pengembangan ilmu pengetahuan, khususnya dalam bidang keamanan digital dan privasi pengguna.

REFERENCES

Armaidianti, W., Lastono, A. S. B., Putra, F. R., Ghozi, I. A., & Rakhmawati, N. A. (2024). Analisis sentimen netizen terhadap personal branding Elon Musk pada platform X dengan pendekatan analisis support vector machine. *Fountain of Informatics Journal*, 9(1), 36-43.

Cahyadi, F., & Rakhmawati, N. A. (2024). *Evaluation of the validation process of prospective recipients of educational scholarships on the Siaplah platform: A case study at the West Kalimantan Provincial Education and Youth Office. Indonesian Journal of Social Technology*, 5(10), 4435.

Refaldi, D. A., Faiz, A., Jawakory, M. R., & Rakhmawati, N. A. (2024). Analisis korelasi Pearson faktor pengaruh generative AI terhadap kemampuan berpikir kritis mahasiswa ITS Surabaya. Jurnal Sistem Informasi dan Aplikasi

(JSIA), 2(2), 9-19.

Wiradharma, P. P., Amartika, N., Dewi, K. M. K., & Rakhmawati, N. A. (2024). Dampak anonimisasi melalui Menfess@ Fess10November terhadap transparansi dan kebebasan berpendapat di platform X. Jurnal Sosial dan Teknologi Terapan AMATA, 3(2), 35-43.

Bonneau, J., Herley, C., Van Oorschot, P. C., & Stajano, F. (2012). *The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. IEEE Symposium on Security and Privacy*, 44. https://doi.org/10.1109/SP.2012.44

Johnson, M., Smith, A., & Lee, K. (2021). *Understanding user behavior and risks in online password managers. Journal of Cybersecurity Research*, 34(2), 105–120. https://doi.org/10.1016/j.jcyber.2021.02.005

Westin, A. F. (1967). *Privacy and freedom. New York: Atheneum.*

Williams, S. (2021). *Risks and benefits of password managers: A user-centered perspective. Cybersecurity in Practice,* 12(3), 123–138. https://doi.org/10.1080/12345678.2021.987654

ISO/IEC 27001. (2013). *Information Security Management Systems — Requirements. International Organization for Standardization.*

Sharma, R., & Kumar, P. (2020). *Evaluating security vulnerabilities in browser-based password managers. In Proceedings of the International Conference on Cyber Security* (pp. 45–52). https://doi.org/10.1109/ICCS.2020.123456