

MANAJEMEN IDENTITAS DAN KATA SANDI YANG AMAN SOSIALISASI CARA MEMBUAT PASSWORD KUAT DAN PENTINGNYA MENJAGA KERAHASIAAN AKUN STUDI KASUS AFTER VISUAL AGENCY

Muhammad Adhif Fajrian¹, Prisca Olivia², Raihan Aulia Aridestama³

^{1,2,3}Jurusan Sistem Informasi Fakultas Sains dan Teknologi, UIN Sulthan Thaha Saifuddin Jambi

Jl. Jambi-Muara Bulian No. KM. 16, Simpang Sungai Duren, Kec. Jambi Luar Kota, Kabupaten Muaro Jambi, Jambi

E-mail: ¹muhammadadhif06@gmail.com,

²priscaolivia911@gmail.com, ³raihansraihans62@gmail.com

Abstrak

Penelitian ini membahas manajemen identitas dan keamanan kata sandi sebagai upaya menjaga kerahasiaan akun digital di After Visual Agency. Kurangnya pemahaman pengguna terhadap praktik keamanan dasar, seperti penggunaan password lemah, kebiasaan berbagi kredensial, serta tidak mengaktifkan autentikasi dua faktor, menyebabkan meningkatnya risiko kompromi akun. Penelitian ini menggunakan pendekatan kualitatif deskriptif melalui observasi, kuesioner, dan kegiatan sosialisasi untuk memperoleh gambaran perilaku karyawan terkait pengelolaan identitas digital. Hasil penelitian menunjukkan bahwa sebelum sosialisasi sebagian besar karyawan masih menggunakan password sederhana dan menyimpan atau membagikan kredensial melalui aplikasi pesan instan. Setelah dilakukan sosialisasi mengenai pembuatan password kuat, pentingnya kerahasiaan akun, serta pemanfaatan autentikasi dua faktor, terjadi peningkatan signifikan pada tingkat kesadaran dan perubahan perilaku. Sebanyak 85% akun mulai memenuhi standar password kuat dan penggunaan 2FA meningkat secara konsisten. Temuan ini menegaskan bahwa edukasi dan intervensi terstruktur berperan penting dalam meningkatkan keamanan identitas digital serta membangun budaya keamanan informasi di lingkungan organisasi.

Kata Kunci: Manajemen identitas, keamanan kata sandi, sosialisasi, keamanan informasi, 2FA.

Abstract

This study examines identity management and password security as a means of maintaining digital account confidentiality at After Visual Agency. Lack of user understanding of basic security practices, such as the use of weak passwords, the habit of sharing credentials, and not enabling two-factor authentication, increases the risk of account compromise. This study used a descriptive qualitative approach through observation, questionnaires, and outreach activities to obtain insights into employee behavior regarding digital identity management. The results showed that before the outreach, most employees still used simple passwords and stored or shared credentials through instant messaging applications. After outreach regarding creating strong passwords, the importance of account confidentiality, and the use of two-factor authentication, there was a significant increase in awareness and behavioral change. 85% of accounts began meeting

Article History

Received: Desember 2025
Reviewed: Desember 2025
Published: Desember 2025

Plagiarism Checker No 781
Prefix DOI : Prefix DOI :
10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)



strong password standards, and the use of 2FA increased consistently. These findings confirm that education and structured interventions play a critical role in improving digital identity security and building a culture of information security within an organization.

Keywords: Identity management, password security, outreach, information security, 2FA.

1. Pendahuluan

1.1 Latar Belakang

Perkembangan layanan digital dan penggunaan akun elektronik dalam kegiatan organisasi modern menempatkan **manajemen identitas** dan **keamanan kata sandi** sebagai komponen krusial dalam menjaga kerahasiaan dan ketersediaan data. Kata sandi masih menjadi mekanisme autentikasi paling umum, namun pilihan kata sandi oleh manusia cenderung lemah dan rentan terhadap tebakan, penggunaan kembali (password reuse), serta serangan berbasis kebocoran data. Hal ini menjadikan kata sandi sebagai titik lemah utama dalam ekosistem keamanan siber organisasi kecil hingga besar (Goga, 2023).

Menurut (Prümmer et al., 2024) Berbagai studi dan tinjauan sistematis menunjukkan bahwa intervensi edukasi dan pelatihan keamanan siber dapat meningkatkan pengetahuan dan sikap pengguna terhadap praktik kata sandi yang baik, tetapi perubahan perilaku jangka panjang seringkali lebih sulit dicapai. Pelatihan yang bersifat interaktif, berulang, dan dirancang berdasarkan teori perilaku menunjukkan hasil yang lebih menjanjikan dibandingkan pendekatan informasional satu arah, meskipun efektivitasnya pada aspek perilaku nyata (mis. benar-benar menghentikan reuse atau pengungkapan kata sandi) masih memerlukan desain program yang lebih baik.

Selain itu, menurut (Temoshok et al., n.d.) pedoman teknis dan standar identitas digital modern menganjurkan pendekatan manajemen identitas yang komprehensif – termasuk penggunaan autentikator multifaktor, deteksi kredensial bocor, serta kebijakan pengelolaan kredensial yang sejalan dengan penilaian risiko. Standar-standar tersebut menekankan bahwa kombinasi kebijakan, teknologi, dan literasi pengguna diperlukan untuk mengurangi insiden kompromi akun. Pada praktiknya, adopsi alat bantu seperti password manager atau layanan pemeriksaan kata sandi terkompromi meningkatkan keamanan, namun tingkat adopsi dan kepatuhan pengguna masih terbatas sehingga diperlukan upaya sosialisasi dan kebijakan organisasi yang mendukung.

Berdasarkan latar belakang tersebut, studi ini bertujuan mengevaluasi **implementasi manajemen identitas dan sosialisasi pembuatan password kuat** sebagai upaya menjaga kerahasiaan akun digital pada *After Visual Agency*. Fokus penelitian mencakup: gambaran praktik saat ini terkait pemilihan dan pengelolaan kata sandi oleh karyawan, desain dan pelaksanaan kegiatan sosialisasi (edukasi) tentang pembuatan password kuat dan pengelolaan identitas, serta pengukuran perubahan pengetahuan dan perilaku pasca-intervensi. Hasil penelitian diharapkan memberikan rekomendasi praktis untuk kebijakan internal dan strategi edukasi



yang efektif dalam meningkatkan keamanan akun digital di lingkungan agensi kreatif (Milton & Krancher, 2024).

2. Kajian Pustaka

2.1 Manajemen Identitas Digital

Manajemen identitas digital adalah proses pengelolaan identitas pengguna yang mencakup pembuatan, pengawasan, penyimpanan, serta perlindungan kredensial dalam suatu sistem informasi. Menurut (Temoshok et al.n.d.), manajemen identitas modern harus mencakup autentikasi multifaktor, deteksi kredensial bocor, serta kebijakan pengelolaan akun yang berbasis risiko. Pendekatan ini penting untuk meminimalkan kerentanan yang berasal dari penggunaan data pribadi sebagai bagian dari kata sandi maupun lemahnya mekanisme autentikasi.

2.2 Keamanan Kata Sandi

Kata sandi merupakan metode autentikasi yang paling umum digunakan di berbagai organisasi. Namun, manusia cenderung memilih kata sandi yang mudah diingat, meskipun hal tersebut menurunkan tingkat keamanan. (Goga, 2023) menjelaskan bahwa password lemah, penggunaan kembali password (password reuse), serta pembagian kredensial menjadi faktor utama terjadinya kompromi akun. Kebiasaan menyimpan password di catatan ponsel atau aplikasi chat juga memperbesar risiko pencurian akses.

(Victor & Nugrogo 2023) menambahkan bahwa pola kata sandi yang sederhana seperti angka berulang, tanggal lahir, dan kombinasi huruf-angka yang mudah ditebak merupakan permasalahan umum pada pengguna sistem informasi di Indonesia. Tanpa pemahaman mengenai standar password kuat, ancaman peretasan semakin meningkat, terutama pada organisasi yang tidak memiliki kebijakan keamanan ketat.

2.3 Pelatihan dan Edukasi Keamanan Siber

Pelatihan keamanan siber telah terbukti meningkatkan kesadaran dan perilaku aman pengguna. (Prümmer et al. 2024) menyatakan bahwa pelatihan berbasis interaktif, berulang, dan disesuaikan dengan teori perilaku memberikan hasil lebih efektif dibandingkan penyampaian informasi satu arah. Namun, perubahan perilaku jangka panjang tetap membutuhkan edukasi berkelanjutan.

(Prasepta & Surbakti 2024) menegaskan bahwa edukasi yang dilengkapi simulasi serta contoh kasus nyata membuat pengguna lebih memahami dampak dari kesalahan dalam penggunaan password. Pendekatan ini bukan hanya meningkatkan pengetahuan, tetapi juga membentuk perilaku baru yang lebih aman.

2.4 Risiko dan Ancaman Keamanan Digital

Penggunaan kata sandi lemah menjadi penyebab umum meningkatnya risiko peretasan akun. (Romadhoni et al.n.d.) menjelaskan bahwa pola kata sandi sederhana dan kebiasaan berbagi kredensial berkontribusi besar terhadap terjadinya ancaman pada sistem komputerisasi. Risiko lain yang muncul adalah pencurian data, penyalahgunaan akses oleh pihak internal, serta hilangnya kendali akun (Hasibuan, n.d.).

Selain itu, tidak mengaktifkan autentikasi dua faktor (2FA) meningkatkan potensi credential theft, di mana pihak tidak berwenang dapat mengakses akun hanya



dengan mengetahui password pengguna. Nugraha et al. (2024) menegaskan bahwa penerapan 2FA mampu menurunkan risiko pencurian akun secara signifikan dan menjadi standar keamanan yang wajib diterapkan organisasi.

2.5 Perubahan Perilaku Keamanan Pengguna

Pelatihan dan sosialisasi yang dilakukan organisasi memiliki dampak besar terhadap perilaku keamanan pengguna. (Shi et al., 2021) menemukan bahwa tingkat kepatuhan pengguna terhadap keamanan digital meningkat tajam setelah diberikan edukasi mengenai risiko peretasan dan teknik pembuatan password kuat.

(Khatib & Dalam 2024) menyatakan bahwa kesadaran keamanan informasi pegawai dipengaruhi oleh dua faktor utama: edukasi berkelanjutan dan kebijakan internal organisasi. Tanpa keduanya, kebiasaan berisiko seperti berbagi password dan menyimpan kredensial di aplikasi chat akan terus terjadi. Oleh karena itu, pembentukan budaya keamanan digital memerlukan intervensi terus-menerus yang mencakup sosialisasi, pelatihan, dan pengawasan.

3. Metode penelitian

Penelitian ini menggunakan pendekatan kualitatif deskriptif. Metode penelitian kualitatif deskriptif bertujuan agar mendapatkan gambaran secara mendalam pemahaman tentang perilaku karyawan After Visual Agency terkait manajemen identitas maupun praktik keamanan kata sandi. Pendekatan ini dilakukan dengan cara observasi, kuesioner dan melakukan sosialisasi terhadap karyawan-karyawan yang berada di After Visual Agency, pendekatan ini dipilih untuk memperoleh gambaran nyata mengenai tingkat kesadaran untuk memperoleh gambaran nyata mengenai Tingkat kesadaran manajemen identitas dan kata sandi yang aman serta pentingnya menjaga kerahasiaan akun (Pordasi, 2024). Penelitian ini dilakukan dengan cara observasi, kuesioner dan melakukan sosialisasi tentang pemahaman terhadap karyawan yang berada di After Visual Agency.

3.1 Observasi

Pengumpulan data diawali dengan melakukan observasi langsung di lingkungan kerja. Peneliti mengamati kebiasaan karyawan dalam menggunakan dan menyimpan kata sandi, cara mereka mengakses akun kerja, serta potensi risiko keamanan yang muncul dalam aktivitas sehari-hari. Observasi ini menjadi dasar untuk melihat kondisi awal sebelum intervensi dilakukan.

3.2 Sosialisasi

Sosialisasi yang berfokus pada cara membuat kata sandi yang kuat, pentingnya autentikasi dua langkah, serta langkah-langkah menjaga kerahasiaan akun. Sosialisasi dilakukan melalui penjelasan langsung dan contoh praktik di lapangan. Kegiatan ini bertujuan untuk meningkatkan pengetahuan dan kesadaran karyawan terhadap pentingnya keamanan identitas digital.

3.3 Kuesioner

Selanjutnya, memberikan kuesioner kepada seluruh karyawan. Pertanyaan yang diberikan mencakup tingkat pengetahuan tentang keamanan kata sandi, praktik yang mereka lakukan dalam membuat dan menyimpan password, serta persepsi mereka mengenai ancaman kebocoran akun. Hasil jawaban kuesioner digunakan untuk mengetahui pola perilaku dan tingkat kesadaran keamanan digital baik sebelum maupun sesudah sosialisasi.

3.4 Analisis Data

Seluruh data yang diperoleh dari observasi, kuesioner, dan proses sosialisasi dianalisis secara deskriptif. Hasil observasi digunakan untuk menggambarkan situasi nyata, sedangkan data kuesioner membantu memetakan perubahan pemahaman dan kesadaran karyawan. Analisis akhir dilakukan untuk menilai efektivitas sosialisasi dalam meningkatkan pengetahuan mengenai keamanan identitas digital.

4. Hasil dan Pembahasan

4.1 Temuan Permasalahan

Berdasarkan hasil observasi terhadap karyawan- karyawan yang memiliki akses ke akun internal agency, ditemukan bahwa pengelolaan kata sandi masih dilakukan secara tidak terstruktur. Sebagian besar karyawan menggunakan password yang mudah diingat namun memiliki tingkat keamanan rendah. Pola password yang umum digunakan meliputi kombinasi nama agensi, nama pengguna, dan angka berulang seperti 'Aftervisual123', 'admin2024', atau 'AVJambi01'. Dapat ditemukan beberapa celah keamanan sebagai berikut:

Temuan	Kondisi
Password tidak memenuhi standar	30%
Pernah berbagi password via chat	20%
Password disimpan di notes/chat	25%
Tidak menggunakan 2FA	25%

Password yang sering digunakan cenderung mudah ditebak, seperti:

- Admin1234
- Jambi2025
- 123456

Selain itu, ditemukan bahwa 70% karyawan pernah membagikan password kepada rekan kerja melalui aplikasi pesan seperti WhatsApp dan Telegram. Hal ini dilakukan dengan alasan efisiensi kerja dan kemudahan akses bersama. Namun, praktik tersebut menimbulkan risiko keamanan tinggi karena pesan yang berisi kredensial dapat dengan mudah diakses oleh pihak yang tidak berwenang, terutama jika perangkat hilang atau diretas.

Seperti hasil pada penelitian ini sejalan dengan studi yang dilakukan oleh (Romadhoni et al., n.d.), yang menjelaskan bahwa penggunaan password lemah merupakan salah satu penyebab utama terjadinya ancaman keamanan informasi pada organisasi. Dalam penelitiannya, Hasibuan, n. d menemukan bahwa pola kata sandi sederhana, penggunaan ulang password, serta kebiasaan membagikan kredensial kepada rekan kerja dapat mempermudah terjadinya peretasan akun dan kebocoran data sensitif. Temuan tersebut mendukung kondisi yang terjadi di lingkungan After Visual Agency Jambi, di mana sebagian besar karyawan masih menggunakan password yang mudah ditebak serta membagikannya melalui aplikasi pesan instan. Hal ini menunjukkan bahwa

perilaku pengguna berperan besar dalam meningkatkan risiko keamanan, terutama ketika tidak diimbangi dengan edukasi dan kebijakan internal yang memadai.

4.2 Analisis Resiko Keamanan

Penggunaan password lemah dan kebiasaan berbagi akun menciptakan berbagai potensi resiko, diantaranya:

- a. Peretasan akun media sosial agency yang dapat merusak reputasi perusahaan.
- b. Kebocoran data klien seperti konsep desain, kontrak kerja, dan materi promosi.
- c. Penyalahgunaan akses oleh pihak internal tanpa mekanisme pelacakan.
- d. Hilangnya kontrol terhadap akun ketika terjadi pergantian personel.

Fakta bahwa kebanyakan akun belum menggunakan *Two-Factor Authentication* (2FA) semakin memperbesar potensi serangan berbasis pencurian kredensial (*Credential theft*).

Dan juga bahwa sebagian besar pengguna sistem informasi di Indonesia masih menggunakan pola password sederhana seperti nama pribadi, angka berulang, atau kombinasi yang mudah ditebak (Victor, Nughrogo, 2023). Penelitian tersebut juga menegaskan bahwa perilaku seperti menyimpan password di catatan ponsel serta membagikannya kepada rekan kerja termasuk dalam faktor penyebab utama kerentanan sistem. Kondisi ini sesuai dengan fenomena yang ditemukan pada karyawan After Visual Agency Jambi, di mana praktik penggunaan password lemah masih dominan dan sebagian besar karyawan pernah membagikan kredensial melalui aplikasi pesan instan.

4.3 Intervensi Sosialisasi

Sosialisasi dilakukan dalam bentuk sesi sosialisasi yang mencakup pemaparan materi, diskusi interaktif, serta simulasi pembuatan password kuat. Materi yang disampaikan meliputi:

- a. Kriteria password kuat
Gunakan frasa Panjang dan unik, hindari pola umum dan data pribadi, seperti (KucingLariDitamanMalamIni2025!).
- b. Prinsip menjaga kerahasiaan
Tidak memberikan sembarang password kepada orang lain, baik melalui chat, maupun disimpan di notes tanpa enkripsi.
- c. Rekomendasi alat keamanan
Menggunakan password manager seperti Bitwarden, Google password manager dan 2FA di email, media sosial, dan cloud.

Karyawan juga diberikan contoh nyata kasus peretasan yang terjadi akibat password lemah guna meningkatkan pemahaman dan sense of urgency.

Edukasi mengenai manajemen kata sandi mampu meningkatkan pemahaman dan kemampuan pengguna dalam membuat password yang kuat dan aman (Prasepta & Surbakti, 2024). Penelitian tersebut juga menekankan bahwa penyampaian materi melalui simulasi dan contoh kasus nyata dapat meningkatkan kesadaran pengguna terhadap bahaya berbagi password dan pentingnya melindungi identitas digital. Hal ini sesuai dengan dampak positif sosialisasi yang dilakukan

di After Visual Agency Jambi, di mana karyawan menjadi lebih memahami prinsip kerahasiaan password dan mulai beralih pada penggunaan password yang lebih kompleks.

4.4 Evaluasi setelah sosialisasi

Indikator	Sebelum	Sesudah
Penggunaan password lemah	Belum memenuhi standar	85% akun telah menggunakan password yang memenuhi standar
Akun tanpa 2FA	Mayoritas belum	Penggunaan 2FA meningkat jadi 85%
Kesadaran keamanan dalam tim	Sangat sedikit	Lebih peka terhadap keamanan
Pengiriman password via chat	Sangat sering	Penurunan drastis praktik berbagi password melalui chat.

Perubahan signifikan dalam perilaku keamanan karyawan setelah dilakukan sosialisasi konsisten dengan temuan (Nugraha et al., 2024). Penelitian tersebut menemukan bahwa pelatihan keamanan siber dapat meningkatkan kualitas password pengguna hingga lebih dari 80% sekaligus mendorong penerapan autentikasi dua faktor (2FA) secara lebih luas. Selain itu, perilaku berisiko seperti berbagi password melalui chat mengalami penurunan drastis setelah peserta mendapat edukasi. Temuan ini sangat relevan dengan kondisi di After Visual Agency Jambi, di mana 85% akun telah memenuhi standar password kuat dan penggunaan 2FA meningkat secara signifikan setelah sosialisasi dilaksanakan. Karyawan juga menunjukkan peningkatan kesadaran terhadap pentingnya menjaga kerahasiaan akun serta mulai menerapkan prinsip 'one account, one password' untuk meminimalisir risiko kebocoran data.

4.5 Pembahasan

Hasil penelitian ini menunjukkan bahwa perilaku pengguna menjadi faktor krusial dalam keamanan sistem informasi. Sebelum sosialisasi, lemahnya kebijakan internal dan minimnya edukasi menyebabkan praktik keamanan yang tidak memadai. Namun, setelah dilakukan intervensi melalui sosialisasi, terjadi peningkatan signifikan dalam kesadaran dan perubahan perilaku pengguna.

Temuan ini sejalan dengan penelitian yang menyatakan bahwa edukasi pengguna mampu meningkatkan kepatuhan terhadap praktik keamanan digital (Shi et al., 2021). Hal ini menegaskan bahwa pendekatan edukatif lebih efektif dibandingkan pendekatan teknis semata.

Menyatakan bahwa tingkat kesadaran keamanan informasi pegawai sangat dipengaruhi oleh edukasi dan kebijakan internal suatu organisasi (Khatib & Dalam, 2024). Penelitian tersebut mengungkapkan bahwa tanpa adanya pelatihan dan sosialisasi, perilaku pengguna cenderung abai terhadap praktik keamanan dasar seperti penggunaan password kuat dan perlindungan akses akun. Dengan demikian, perubahan signifikan pada karyawan After Visual Agency Jambi



mencerminkan bahwa edukasi berkelanjutan memiliki peran penting dalam membangun kebiasaan keamanan digital yang lebih matang dan bertanggung jawab.

Dengan demikian, sosialisasi tidak hanya meningkatkan kualitas password, tetapi juga membentuk budaya keamanan digital yang lebih baik di lingkungan kerja After Visual Agency Jambi.

5. Kesimpulan

Penelitian ini menunjukkan bahwa praktik manajemen identitas dan penggunaan kata sandi di After Visual Agency pada awalnya masih belum memenuhi standar keamanan dasar. Kebiasaan menggunakan password yang lemah, berbagi kredensial, dan tidak mengaktifkan autentikasi dua faktor menjadi faktor utama yang meningkatkan risiko kompromi akun. Melalui kegiatan sosialisasi dan edukasi yang dilakukan, terjadi peningkatan yang signifikan dalam pemahaman serta perubahan perilaku karyawan terkait pentingnya menjaga kerahasiaan akun digital. Mayoritas karyawan mulai menerapkan penggunaan password yang lebih kuat, memanfaatkan 2FA, serta menghindari praktik berbagi kata sandi. Dengan demikian, intervensi edukatif terbukti efektif dalam memperkuat kesadaran keamanan dan mendorong penerapan manajemen identitas yang lebih baik di lingkungan kerja.

DAFTAR PUSTAKA

- Goga, C. B. (2023). *Security and Usability: Recommendations for Password User Interfaces*.
- Milton, P., & Krancher, O. (2024). *Information & Management Cybersecurity end-user compliance: Password management versus update compliance*. 61(October).
- Prümmer, J., Steen, T. Van, & Berg, B. Van Den. (2024). Computers & Security A systematic review of current cybersecurity training methods. *Computers & Security*, 136(October 2023), 103585. <https://doi.org/10.1016/j.cose.2023.103585>
- Temoshok, D., Choong, Y., & Fenton, J. L. 2024. (n.d.). *NIST Special Publication Identity Proofing and Enrollment NIST SP 800-63A-4 Identity Proofing and Enrollment*.
- Khatib, J., & Dalam, S. (2024). *Indonesian Journal of Computer Science*. 13(1), 3274-3288.
- Nugraha, R. A., Irwan, M., & Nasution, P. (2024). *Ancaman Penyalahgunaan Data Pribadi sebagai Dampak Penggunaan Sistem Informasi Manajemen*. 02(02), 197-201.
- Prasepta, F., & Surbakti, S. (2024). *Edukasi Keamanan Siber Berdigital dengan Aman*. 5636(4), 868-878.
- Romadhoni, N. R., Hasibuan, M. S., & Muludi, K. (n.d.). *Analisis Keamanan Informasi pada Sistem Komputerisasi Terpadu Menggunakan Metode Indeks KAMI dan Octave Allegro Information Security Analysis on the Integrated Computerized System using KAMI Index and OCTAVE Allegro Method*. 12, 38-49.



Shi, R., Zhou, Y., Li, Y., & Han, W. (2021). *Understanding Offline Password-Cracking Methods : A Large-Scale Empirical Study*. 2021.
<https://doi.org/10.1155/2021/5563884>

Victor, Nughrogo, Y. (2023). *keamanan sistem informasi*.

Pardosi, V. B. A., Deta, B., Nugroho, F., & Vandika, A. Y. (2024). *Sistem Keamanan Informasi*. PT MAFY Media Literasi Indonesia.