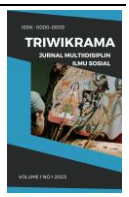
Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 8 2025
E-ISSN: 2988-1986
Open Access:



PENINGKATAN KESADARAN KEAMANAN DIGITAL MELALUI SOSIALISASI MANAJEMEN IDENTITAS DAN PENGGUNAAN KATA SANDI AMAN PADA MAHASISWA UIN STS JAMBI

Alfarizi[1], Indriyani Saputri[2], Jeki Gusma Irawan[3]
Sistem Informasi, Universitas Islam Negeri Sultan Thaha Saifuddin Jambi

ARTICLE INFO

Article history:
Received November 2025
Revised November 2025
Accepted November 2025
Available online November 2025

Email:
[1]alfarizi302004@gmail.com ,
[2]indriiiieaan@gmail.com
[3]jekigusmairawan12@gmail.com

Abstrak

Kegiatan sosialisasi ini bertujuan untuk meningkatkan kesadaran mahasiswa baru UIN STS Jambi terhadap pentingnya manajemen identitas digital dan penggunaan kata sandi yang aman dalam aktivitas daring. Kegiatan dilaksanakan di kampus UIN STS Jambi dengan metode presentasi interaktif, diskusi, dan tanya jawab. Materi mencakup pengenalan identitas digital, risiko keamanan siber, cara membuat kata sandi yang kuat, penggunaan aplikasi password manager, serta penerapan verifikasi dua langkah (2FA). Berdasarkan hasil kuesioner yang dibagikan kepada peserta, mayoritas mahasiswa memahami pentingnya keamanan digital dan setuju bahwa edukasi semacam ini perlu dilakukan secara rutin. Kegiatan ini diharapkan dapat menumbuhkan kebiasaan aman dalam penggunaan akun digital di kalangan mahasiswa.

Kata kunci: Manajemen Identitas, Keamanan Digital, Kata Sandi, Sosialisasi, Mahasiswa

1. Pendahuluan

Perkembangan teknologi digital belakangan ini benar-benar mengubah cara orang beraktivitas. Hampir semuanya sekarang serba online mulai dari belajar, kerja, ngobrol, sampai ngurus layanan pemerintahan pun sudah pindah ke aplikasi. Kemudahan ini memang bikin hidup jadi lebih praktis, tapi di sisi lain muncul juga masalah baru yang nggak bisa dianggap remeh, yaitu soal keamanan identitas digital. Data pribadi yang dulu cuma ada di dompet atau di lemari, sekarang ikut tersimpan di berbagai platform digital, entah itu akun media sosial, aplikasi belanja, sampai layanan keuangan.

Masalahnya, makin banyak data yang tersebar, makin besar juga kemungkinan terjadi penyalahgunaan. Kasus seperti kebocoran data, peretasan akun, penipuan online, dan pencurian identitas digital sudah sering terdengar. Banyak orang mungkin merasa hal seperti itu jauh dari dirinya, padahal sebagian besar kasus terjadi justru karena hal sepele: kata sandi mudah ditebak, pakai satu password untuk semua akun, atau asal klik link yang kelihatannya normal. Ujung-ujungnya, akun diretas tanpa sadar dan data pribadi ikut bocor.

Di sinilah pentingnya manajemen identitas digital. Ini bukan cuma soal login atau sekadar mengingat password, tapi bagaimana seseorang mengelola identitasnya di dunia digital supaya tetap aman. Mulai dari cara membuat kata sandi yang benar, penggunaan alat pengamanan tambahan seperti verifikasi dua langkah, sampai paham mana tindakan yang aman dan mana yang berisiko. Banyak penelitian menunjukkan bahwa teknologi keamanan canggih tidak akan bekerja maksimal kalau penggunanya sendiri tidak sadar risiko.

Sayangnya, literasi keamanan digital di Indonesia masih cukup rendah. Tidak sedikit pengguna yang menganggap keamanan adalah tugas penyedia layanan saja, padahal sebagian besar kebocoran justru dipicu oleh kelalaian pengguna. Hal-hal sederhana seperti membagikan kode OTP, menggunakan WiFi publik tanpa perlindungan, atau menyimpan kata sandi di

catatan ponsel bisa membuka peluang terjadinya pencurian identitas digital. Karena itu, memahami cara mengelola identitas digital menjadi keterampilan penting di tengah perkembangan teknologi yang semakin cepat.

Melihat kondisi tersebut, pembahasan mengenai manajemen identitas digital, pengelolaan kata sandi, penerapan verifikasi dua langkah, serta tingkat kesadaran pengguna menjadi sangat relevan. Keempat aspek ini saling berkaitan dan berkontribusi besar dalam menjaga keamanan akun digital seseorang. Dengan memahami dasar-dasarnya, pengguna bisa lebih siap menghadapi potensi ancaman digital dan mengurangi risiko penyalahgunaan data pribadi. Selain itu, pembahasan ini juga bisa menjadi dasar untuk perbaikan keamanan baik bagi pengguna maupun penyedia layanan.

2. Landasan Teori

A. Manajemen Identitas Digital

Manajemen identitas digital sebenarnya menjadi bagian penting dari aktivitas kita sehari-hari, meskipun banyak orang tidak menyadarinya. Setiap kali seseorang membuat akun baru, mengunggah data pribadi, atau masuk ke suatu layanan dengan username dan password, saat itu juga ia sedang membangun identitas digitalnya. Identitas ini tidak hanya berisi nama pengguna atau email, tetapi juga bisa mencakup jejak aktivitas, preferensi, hingga data-data yang secara tidak langsung menggambarkan kebiasaan seseorang ketika menggunakan layanan digital.

Menurut Rihan, Priharsari, dan Hanggara (2022), identitas digital merupakan representasi dari diri seseorang yang digunakan untuk mendapatkan akses ke layanan daring. Artinya, identitas ini memiliki nilai penting karena berkaitan langsung dengan akses seseorang terhadap berbagai platform. Dalam konteks Indonesia sendiri, isu mengenai identitas digital makin relevan setelah pemerintah mulai mendorong penerapan identitas kependudukan digital dan sistem layanan publik berbasis teknologi. Suminar dan Nugroho (2023) menjelaskan bahwa pengelolaan identitas digital membutuhkan dukungan dari regulasi, infrastruktur, dan sistem keamanan yang kuat agar pengguna terlindungi dari penyalahgunaan data.

Jika manajemen identitas digital tidak dijalankan dengan benar, risiko seperti pencurian identitas, penyalahgunaan akun, hingga kebocoran informasi pribadi menjadi lebih besar. Karena itu, manajemen identitas digital tidak lagi dianggap sebagai isu teknis semata, tetapi sudah menjadi kebutuhan mendasar di era di mana hampir semua aspek kehidupan terhubung dengan teknologi.

B. Manajemen Kata Sandi

Kata sandi sering dianggap sepele, padahal inilah “kunci rumah digital” seseorang. Banyak insiden keamanan justru terjadi bukan karena sistem yang buruk, tetapi karena kesalahan penggunanya sendiri. Misalnya, memakai kata sandi yang terlalu sederhana, menggunakan kombinasi yang sama untuk banyak akun, atau membagikan kata sandi

kepada orang lain tanpa mempertimbangkan risiko. Hal-hal seperti ini sering dianggap wajar, padahal bisa membuka peluang terjadinya peretasan.

Komalasari (2018) menyoroti bahwa rendahnya kesadaran pengguna dalam membuat kata sandi yang kuat menjadi salah satu penyebab meningkatnya kasus peretasan akun. Pengguna cenderung menggunakan kata sandi yang mudah ditebak, seperti tanggal lahir atau nama hewan peliharaan, sehingga sangat rentan terhadap serangan brute force ataupun teknik rekayasa sosial. Sementara itu, penelitian Alodhyani, Theodorakopoulos, dan Reinecke (2020) menunjukkan bahwa penggunaan password manager dapat menjadi solusi praktis. Alat ini membantu membuat dan menyimpan kata sandi yang kompleks tanpa membebani daya ingat pengguna.

Dengan semakin banyaknya akun digital yang dimiliki seseorang, manajemen kata sandi yang baik bukan hanya sekadar rekomendasi, tetapi merupakan kebutuhan. Tanpa pengelolaan yang tepat, kata sandi bisa menjadi titik masuk bagi penyusup untuk mengambil alih identitas digital seseorang. Oleh karena itu, kebiasaan kecil seperti rutin mengganti password, tidak mudah percaya pada tautan mencurigakan, dan memanfaatkan password manager dapat memberikan perlindungan tambahan yang signifikan.

C. Verifikasi Dua Langkah (2FA)

Di tengah maraknya kasus pencurian akun, penggunaan verifikasi dua langkah atau 2FA menjadi salah satu cara paling efektif untuk menambah lapisan keamanan. Sistem ini bekerja dengan meminta pengguna melakukan dua bentuk verifikasi yang berbeda, seperti memasukkan kata sandi dan kode OTP yang dikirim melalui SMS atau aplikasi autentikasi. Dengan metode seperti ini, meskipun kata sandi seseorang berhasil dicuri, akun tetap sulit dibobol karena penyusup tidak memiliki akses ke langkah verifikasi kedua.

Saputra dan Rahman (2024) menemukan bahwa penerapan 2FA dapat secara signifikan mengurangi risiko pembobolan akun digital. Namun, meskipun metode ini terbukti efektif, tingkat penerapannya masih belum merata. Banyak pengguna merasa proses verifikasi tambahan itu merepotkan atau mengganggu kenyamanan saat login. Padahal jika dilihat dari risiko yang ada, melakukan satu langkah tambahan untuk keamanan jauh lebih baik daripada menghadapi akibat dari akun yang diretas.

Dengan semakin meningkatnya kasus kejahatan siber, penggunaan 2FA seharusnya tidak lagi dianggap pilihan, tetapi menjadi standar baru dalam menjaga identitas digital. Platform besar seperti Gmail, Meta, dan layanan perbankan pun sudah mendorong penggunanya untuk menggunakan 2FA agar keamanan akun semakin terjamin.

D. Kesadaran Pengguna

Kesadaran pengguna merupakan faktor penentu yang sering kali diabaikan dalam pembahasan keamanan digital. Banyak masalah keamanan sebenarnya terjadi bukan karena sistemnya lemah, tetapi karena penggunanya kurang berhati-hati. Contoh sederhananya seperti lupa mengganti kata sandi, mengklik tautan mencurigakan,

menggunakan WiFi publik tanpa perlindungan, atau membagikan informasi pribadi kepada orang lain tanpa memeriksa kebenaran sumbernya.

Komalasari (2018) menjelaskan bahwa rendahnya pemahaman pengguna mengenai keamanan digital menjadi pemicu utama risiko kebocoran data. Kebiasaan-kebiasaan yang dianggap sepele itu sebenarnya dapat menjadi pintu masuk bagi pelaku kejahatan siber. Sementara itu, Purba dan Mauluddin (2023) menunjukkan bahwa sebagian besar kasus penipuan digital dan pencurian identitas di Indonesia disebabkan oleh kurangnya literasi keamanan dasar.

Oleh karena itu, meningkatkan kesadaran pengguna menjadi langkah penting dalam membangun lingkungan digital yang aman. Teknologi pengamanan seperti password manager atau 2FA tidak akan bekerja maksimal jika penggunanya sendiri tidak memahami risiko yang ada. Dengan pengetahuan yang cukup, pengguna dapat mengambil langkah-langkah sederhana namun efektif untuk melindungi dirinya, seperti mengelola kata sandi dengan baik, berhati-hati dalam memberikan informasi, dan memahami potensi ancaman digital.

3. Metode penelitian

Kegiatan sosialisasi dilaksanakan melalui penyampaian materi secara langsung, diskusi, dan sesi tanya jawab. Peserta kegiatan adalah mahasiswa semester 1 dari berbagai kelas. Sebagai bagian dari evaluasi, peserta mengisi kuesioner yang digunakan untuk mengukur tingkat pemahaman mereka sebelum dan setelah kegiatan berlangsung.

Materi yang disampaikan meliputi:
1. Pengenalan identitas digital
2. Ancaman dan risiko keamanan daring
3. Teknik membuat kata sandi yang kuat
4. Penggunaan password manager
5. Pentingnya verifikasi dua langkah (2FA)
6. Kebiasaan aman dalam aktivitas digital

4. Hasil dan pembahasan

Berdasarkan hasil kuesioner, mahasiswa semester 1 yang mengikuti kegiatan ini sebagian besar merupakan pengguna aktif internet, dengan durasi penggunaan lebih dari enam jam per hari. Hampir semua responden menggunakan media sosial setiap hari, sehingga tingkat risiko paparan ancaman siber cukup tinggi.

Setelah mengikuti sosialisasi, pemahaman mahasiswa tentang keamanan digital menunjukkan peningkatan signifikan. Sekitar 75% responden mengaku lebih memahami pentingnya melindungi identitas digital dan menerapkan kata sandi yang kuat. Meski demikian, masih ditemukan beberapa kebiasaan berisiko, seperti tidak mengganti kata sandi secara berkala dan membagikan kata sandi kepada orang lain.

Pemahaman mahasiswa mengenai fitur verifikasi dua langkah juga meningkat. Banyak yang baru mengetahui manfaat 2FA dari sosialisasi ini dan berniat untuk mengaktifkan fitur tersebut di akun penting seperti email, media sosial, dan layanan akademik.

Triwikrama: Jurnal Ilmu Sosial
Volume 11 No 8 2025
E-ISSN: 2988-1986
Open Access:

Secara umum, peserta memberikan tanggapan positif. Mereka menilai materi yang disampaikan sangat relevan dengan kehidupan digital mereka. Beberapa mengusulkan agar kegiatan seperti ini diadakan secara rutin dengan cakupan materi yang lebih luas, termasuk simulasi ancaman siber.

Kesimpulan

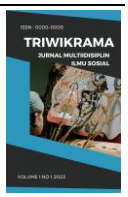
Sosialisasi manajemen identitas digital dan keamanan kata sandi ini berhasil meningkatkan pemahaman mahasiswa mengenai pentingnya menjaga keamanan akun serta data pribadi. Meskipun pemahaman meningkat, beberapa kebiasaan pengguna masih perlu diperbaiki agar praktik keamanan digital dapat diterapkan secara konsisten.

Saran

1. Kegiatan serupa sebaiknya dilakukan secara berkala untuk mahasiswa baru.
2. Mahasiswa dianjurkan mulai membiasakan diri menggunakan password manager dan menerapkan 2FA.
3. Kampus dapat menyediakan program literasi digital jangka panjang sebagai bentuk dukungan terhadap keamanan data civitas akademika

Dokumentasi



Daftar Pustaka

Alodhyani, F., Theodorakopoulos, G., & Reinecke, P. (2020). *Password Managers—It's All about Trust and Transparency*. Future Internet, 12(11), 189.

Komalasari, R. (2018). *Kesadaran akan Keamanan Penggunaan Username dan Password*. Tematik: Jurnal Teknologi Informasi.

Purba, Y. O., & Mauluddin, A. (2023). *Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Studi Potensi Pencurian Data Online*. JCIC: Jurnal CIC.

Rihan, M. K. R., Priharsari, D., & Hanggara, B. T. (2022). *Analisis Kesediaan Berbagi Identitas Digital Berdasarkan Faktor Self-Efficacy, Perceived Severity dan Gender*. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 6(11), 5380–5389.

Saputra, D., & Rahman, T. (2024). *Penerapan Two-Factor Authentication (2FA) sebagai Upaya Pengamanan Akun Digital*. Jurnal Informatika dan Keamanan Siber.

Suminar, L. R., & Nugroho, A. A. (2023). *Adopsi Teknologi Blockchain di Sektor Publik: Peluang Pembentukan Sistem Identitas Digital Nasional di Era VUCA*. Dinamika Governance, 12(4), 81–92.