JURNAL DIKMAS
Volume. 7, Nomor. 1, Juni 2025
e-ISSN: 2830-7836; p-ISSN: 2830-7909, Hal 20-32
DOI :https://doi.org/10.55606/dikmas.v4i2.434
Available Online at: https://jurnal.sttarastamarngabang.ac.id/index.php/DIKMAS

Edukasi Keamanan Digital dalam Penggunaan Dompet Digital di Kalangan Mahasiswa: Upaya Meningkatkan Kesadaran dan Keamanan Transaksi

Digital Security Education in the Use of Digital Wallets among Students: Efforts to Increase Awareness and Transaction Security

Astri Rumondang Banjarnahor
Institut Transportasi dan Logistik (ITL) Trisakti Jakarta, Indonesia

Alamat: Jalan IPN Kebun Nanas No 2, Cipinang Besar, Jatinegara, Jakarta Timur
Korespondensi penulis: rumondangastri@gmail.com

Article History:
Received: November 15, 2022
Accepted: November 30, 2022
Published: Desember 30, 2022

Keywords: *Literacy, Security, Digital, Risk*

Abstract. *This study aims to enhance digital security literacy among Dompet Digital users. With the growing adoption of Dompet Digitals offering transactional convenience, digital security risks have also risen, especially among users with limited data protection awareness. The educational program focuses on introducing digital security risks, such as phishing, malware, and social engineering, along with providing protective strategies like two-factor authentication (2FA) and avoiding unsecured public Wi-Fi networks. The methods employed include socialization sessions, seminars, and workshops designed to build Dompet Digital users' awareness in safeguarding their accounts. The program results indicate a significant increase in users' awareness and practical skills in identifying risks and implementing security measures. Additionally, users are expected to act as change agents, spreading this knowledge within their communities. Regular educational initiatives and collaboration with Dompet Digital providers are also recommended as ongoing steps to maintain digital security.*

Abstrak

Kegiatan ini bertujuan meningkatkan literasi keamanan digital pengguna Dompet Digital dalam penggunaan layanan tersebut. Seiring tingginya adopsi Dompet Digital yang menawarkan kemudahan transaksi, risiko keamanan digital juga meningkat, terutama di kalangan pengguna yang minim pemahaman tentang keamanan data. Program edukasi ini berfokus pada pengenalan risiko keamanan digital, seperti phishing, malware, dan social engineering, serta penyediaan strategi perlindungan seperti penggunaan autentikasi dua faktor (2FA) dan penghindaran jaringan Wi-Fi publik. Metode yang digunakan mencakup sosialisasi, seminar, dan workshop yang dirancang untuk membangun kesadaran pengguna Dompet Digital dalam menjaga keamanan akun mereka. Hasil program menunjukkan peningkatan signifikan dalam kesadaran dan keterampilan praktis pengguna Dompet Digital dalam mengidentifikasi risiko serta menerapkan langkah-langkah keamanan. Selain itu, diharapkan mereka mampu menjadi agen perubahan yang menyebarkan informasi ini di komunitas mereka. Edukasi rutin dan kolaborasi dengan penyedia Dompet Digital juga direkomendasikan sebagai langkah berkelanjutan untuk menjaga keamanan digital.

Kata Kunci: Literasi, Keamanan, Digital, Risiko

1. PENDAHULUAN

Transformasi digital dalam beberapa dekade terakhir telah mengubah tatanan transaksi keuangan global, termasuk di kalangan mahasiswa yang kini semakin banyak menggunakan Dompet Digital sebagai metode pembayaran utama (Herdioko, 2023). Dompet Digital menawarkan kemudahan akses yang signifikan dalam bertransaksi secara

non-tunai, mulai dari membayar makanan di kantin, melakukan pembayaran transportasi, hingga belanja daring. Sifatnya yang cepat dan praktis menjadikannya solusi ideal bagi mahasiswa yang akrab dengan teknologi. Namun, di balik kemudahan ini, Dompet Digital juga membawa berbagai risiko keamanan yang sering kali tidak disadari, terutama di kalangan mahasiswa yang minim pemahaman tentang risiko digital (Hartono, 2023; Inaya, Ismiarti and Nofirda, 2024).

Maraknya penggunaan Dompet Digital di kalangan mahasiswa disebabkan oleh berbagai faktor, mulai dari kemudahan transaksi hingga promosi menarik seperti cashback dan diskon. Hal ini menunjukkan bahwa gaya hidup digital mahasiswa tidak terpisahkan dari transaksi berbasis Dompet Digital (Gunawan and Winarti, 2022). Namun, perubahan ini juga memperlihatkan sisi lain dari teknologi keuangan digital, yaitu ancaman keamanan yang semakin meningkat. Banyak mahasiswa yang belum menyadari bahwa transaksi Dompet Digital tidak sepenuhnya aman dan rentan terhadap berbagai serangan siber, termasuk phishing, malware, hingga pencurian data pribadi. Kecenderungan mahasiswa untuk mengabaikan keamanan digital, baik karena minimnya edukasi atau kepercayaan yang terlalu tinggi pada teknologi, menimbulkan potensi kerugian yang serius (Badri, 2020).

Berbagai modus kejahatan digital sering kali menyasar pengguna Dompet Digital yang kurang berhati-hati. Salah satu modus yang paling umum adalah phishing, yakni penipuan di mana pelaku kejahatan menyamar sebagai institusi terpercaya (seperti bank atau penyedia Dompet Digital) dengan tujuan memperoleh informasi sensitif, seperti kata sandi atau nomor identifikasi pribadi (Hartono, 2023). Phishing biasanya dilakukan melalui email atau pesan yang tampak resmi, lengkap dengan logo dan informasi institusi terkait untuk meyakinkan korban. Pesan ini mengandung tautan palsu yang mengarahkan korban ke halaman web yang mirip dengan situs resmi, di mana mereka diminta untuk memasukkan informasi pribadi. Ketika pengguna tidak waspada dan mengisi informasi tersebut, data mereka dapat dicuri dan digunakan untuk mengakses akun Dompet Digital atau rekening bank mereka .

Selain itu, risiko lain yang perlu diwaspadai adalah malware atau perangkat lunak berbahaya yang bisa masuk ke perangkat pengguna melalui aplikasi atau situs palsu. Malware ini bisa mencuri informasi penting dari perangkat tanpa sepengetahuan pengguna, termasuk kata sandi dan informasi keuangan lainnya. Mengingat semakin banyak mahasiswa yang mengunduh aplikasi tanpa mempertimbangkan sumber atau keamanan aplikasi tersebut, risiko malware semakin meningkat. Oleh karena itu, mahasiswa perlu diajarkan untuk memastikan aplikasi yang mereka unduh berasal dari sumber resmi, seperti

Google Play Store atau App Store, serta memperhatikan ulasan pengguna lainnya sebagai salah satu cara mengecek keamanan aplikasi (Badri, 2020).

Program pengabdian masyarakat yang kami rancang bertujuan untuk menjawab kebutuhan mendesak ini, dengan fokus utama pada pemberian informasi dasar dan strategi keamanan digital, peningkatan literasi keamanan digital, serta membangun kesadaran mahasiswa tentang pentingnya kehati-hatian dalam menggunakan teknologi pembayaran digital. Dalam tulisan ini, akan dibahas tiga tujuan program pengabdian yang mencakup strategi edukasi untuk memastikan mahasiswa memiliki perlindungan yang memadai dalam penggunaan Dompet Digital serta pemahaman tentang implikasi dari setiap transaksi digital yang mereka lakukan.

Langkah dasar lainnya yang penting dipahami mahasiswa adalah penggunaan kata sandi yang kuat dan autentikasi dua faktor (2FA). Kata sandi yang lemah memudahkan peretas untuk masuk ke akun, sementara autentikasi dua faktor bisa menjadi lapisan keamanan tambahan. Dalam hal ini, penggunaan teknologi enkripsi dari penyedia layanan Dompet Digital juga perlu dimanfaatkan, karena ini memungkinkan data yang dikirimkan selama transaksi dilindungi dengan baik (Gunawan and Winarti, 2022).

Menurut Inaya, Ismiarti dan Nofirda (2024) meningkatkan literasi keamanan digital adalah langkah lanjutan yang krusial dalam menghadapi ancaman digital yang terus berkembang. Literasi keamanan digital yang baik melibatkan pemahaman yang lebih dalam mengenai cara kerja sistem keamanan digital, potensi kebocoran data, serta langkah-langkah praktis yang bisa diambil untuk memitigasi risiko-risiko tersebut. Mahasiswa yang memiliki literasi keamanan digital yang memadai tidak hanya mengetahui ancaman yang ada, tetapi juga memahami cara efektif dalam merespon atau menghindari ancaman tersebut.

Untuk meningkatkan literasi keamanan digital, program pengabdian ini akan mencakup pelatihan dan simulasi praktis yang memungkinkan mahasiswa menghadapi berbagai skenario risiko. Melalui simulasi kasus nyata, mahasiswa dapat belajar langsung mengenali ciri-ciri penipuan phishing atau bagaimana menyaring informasi dari aplikasi yang tidak dikenal. Literasi keamanan digital bukan hanya sekadar teori, tetapi juga kemampuan dalam menerapkan langkah-langkah keamanan secara mandiri. Dengan berpartisipasi aktif dalam pelatihan dan simulasi ini, mahasiswa akan lebih memahami pentingnya perlindungan data pribadi, serta mengembangkan kepekaan untuk mengenali aktivitas mencurigakan.

Lebih dari itu, kesadaran yang tinggi akan membuat mahasiswa lebih proaktif dalam menjaga keamanan data mereka. Mahasiswa akan terdorong untuk secara rutin memeriksa

riwayat transaksi mereka, segera melaporkan aktivitas mencurigakan, dan lebih waspada saat menggunakan jaringan Wi-Fi publik. Selain itu, program ini juga menekankan pentingnya saling berbagi informasi terkait ancaman digital yang mereka temui, sehingga tercipta lingkungan kampus yang lebih aman dan tanggap terhadap kejahatan siber.

2. METODE

Program pengabdian masyarakat ini dirancang untuk meningkatkan pemahaman dan kesadaran mahasiswa tentang keamanan digital dalam penggunaan Dompet Digital, mengingat pentingnya perlindungan data dan keuangan pribadi di era digital. Mahasiswa, yang cenderung akrab dengan teknologi, sering kali kurang memahami risiko keamanan yang terkait dengan transaksi digital. Melalui metodologi yang berfokus pada sosialisasi, edukasi, dan praktik langsung, kegiatan ini diharapkan dapat membekali mahasiswa dengan pengetahuan dan keterampilan yang mereka perlukan. Berikut adalah pendekatan metodologi yang diimplementasikan dalam program ini.

Pendekatan Sosialisasi dan Edukasi

Pendekatan sosialisasi dan edukasi dipilih sebagai dasar utama dalam program ini, bertujuan untuk menginformasikan mahasiswa tentang ancaman dan cara perlindungan dalam penggunaan Dompet Digital. Sosialisasi merupakan cara efektif untuk memberikan pengenalan awal mengenai konsep keamanan digital dengan memberikan informasi dasar serta peringatan akan risiko yang mungkin mereka hadapi. Edukasi, di sisi lain, menekankan pada pembelajaran mendalam yang melibatkan konsep-konsep dan langkah-langkah praktis yang lebih detail. Pendekatan sosialisasi ini diimplementasikan dalam bentuk diskusi kelompok dan pemberian materi secara langsung, baik dalam format cetak maupun digital. Mahasiswa diberikan materi berupa panduan keamanan digital, daftar risiko umum, dan cara mengenali tanda-tanda ancaman. Selain itu, edukasi dalam program ini juga mengajak mahasiswa untuk aktif berpartisipasi dalam kegiatan yang diselenggarakan, seperti seminar dan workshop, sehingga mereka tidak hanya menerima informasi secara pasif, tetapi juga terlibat dalam proses pembelajaran yang interaktif.

Penyelenggaraan Seminar atau Webinar mengenai Keamanan Digital dalam Penggunaan Dompet Digital

Untuk meningkatkan pengetahuan mahasiswa tentang keamanan digital, diselenggarakan seminar dan webinar sebagai kegiatan utama dalam program ini. Kegiatan seminar dan webinar ini dilakukan dengan tujuan memperkenalkan mahasiswa pada berbagai jenis ancaman digital, termasuk phishing, malware, dan pencurian data, serta

langkah-langkah preventif yang dapat mereka ambil. Format seminar dan webinar dipilih karena memungkinkan interaksi dua arah antara penyaji dan peserta, yang efektif dalam memberikan pemahaman yang mendalam dan responsif terhadap pertanyaan mahasiswa. Seminar atau webinar dimulai dengan sesi pengantar yang membahas pentingnya menjaga keamanan digital di era transaksi non-tunai. Pembicara dalam kegiatan ini adalah ahli keamanan digital atau praktisi yang berpengalaman dalam industri teknologi keuangan, yang mampu memberikan pandangan mendalam serta studi kasus nyata mengenai risiko yang terkait dengan penggunaan Dompet Digital. Materi dalam seminar meliputi teknik keamanan dasar, cara melindungi akun Dompet Digital, hingga upaya mengenali modus-modus kejahatan seperti phishing. Seminar ini disertai dengan pemutaran video singkat, visualisasi ancaman keamanan digital, serta studi kasus nyata yang menarik perhatian mahasiswa.

Pembuatan Materi Edukasi yang Mudah Diakses, Seperti Pamflet, Poster, atau Video Singkat

Untuk memperkuat pemahaman mahasiswa, program ini juga menyediakan materi edukasi yang dapat diakses dengan mudah dan dapat dijadikan referensi mandiri di luar kegiatan sosialisasi langsung. Materi edukasi ini meliputi pamflet, poster, dan video singkat yang menyajikan informasi keamanan digital dengan cara yang ringkas, menarik, dan mudah dipahami. Materi edukasi ini disusun agar dapat menjangkau mahasiswa di berbagai platform, baik cetak maupun digital, sehingga dapat diakses kapan saja oleh mahasiswa yang membutuhkan panduan tambahan. Pamflet dan poster dibuat dengan desain yang menarik serta bahasa yang sederhana, agar mudah dipahami oleh semua kalangan mahasiswa. Isi materi ini mencakup tips praktis dalam menjaga keamanan akun Dompet Digital, seperti anjuran untuk menggunakan kata sandi yang kuat, menghindari tautan mencurigakan, serta langkah-langkah preventif lain yang dapat diterapkan mahasiswa dalam kehidupan sehari-hari. Pamflet dan poster ini didistribusikan di berbagai area kampus dan juga dalam format digital, yang dibagikan melalui platform media sosial kampus agar dapat diakses lebih luas. mahasiswa yang memiliki waktu terbatas.

Pelaksanaan Workshop Praktis: Kegiatan Praktek Langsung dengan Mahasiswa untuk Mengenalkan Berbagai Fitur Keamanan dalam Dompet Digital

Selain penyampaian informasi, kegiatan ini juga dilengkapi dengan pelaksanaan workshop praktis. Workshop ini bertujuan untuk memberikan pengalaman langsung kepada mahasiswa dalam menggunakan berbagai fitur keamanan pada aplikasi Dompet Digital yang mereka gunakan. Workshop ini difokuskan pada penerapan pengetahuan praktis yang

telah disampaikan dalam seminar dan materi edukasi, dengan memandu mahasiswa dalam menggunakan fitur-fitur keamanan Dompet Digital yang relevan. Dalam workshop ini, mahasiswa diberikan panduan langkah demi langkah mengenai pengaturan keamanan dalam aplikasi Dompet Digital mereka, seperti cara mengaktifkan autentikasi dua faktor (2FA), membuat kata sandi yang kuat, dan mengelola notifikasi untuk transaksi mencurigakan. Dengan praktek langsung ini, mahasiswa dapat merasakan dan memahami secara lebih jelas mengenai fitur keamanan yang tersedia, serta manfaatnya dalam menjaga akun mereka dari potensi serangan.

Simulasi atau Contoh Kasus Penipuan yang Sering Terjadi, serta Cara Menghindarinya

Sebagai bagian dari workshop, mahasiswa diberikan simulasi atau contoh kasus penipuan yang sering terjadi dalam penggunaan Dompet Digital. Simulasi ini meliputi berbagai modus kejahatan digital yang sering terjadi, seperti phishing dan penipuan berbasis sosial engineering, di mana pelaku kejahatan mencoba menipu korban agar memberikan informasi pribadi atau melakukan transfer uang. Dalam simulasi ini, mahasiswa diberikan contoh pesan atau email palsu yang seolah-olah berasal dari penyedia Dompet Digital resmi, dengan permintaan untuk memasukkan data pribadi atau informasi keuangan. Mahasiswa diajak untuk menganalisis pesan tersebut, mengenali tanda-tanda yang menunjukkan bahwa pesan tersebut adalah penipuan, serta mempelajari cara meresponnya dengan tepat. Diskusi mengenai solusi dalam menghadapi setiap kasus juga dilakukan, sehingga mahasiswa dapat mengetahui tindakan pencegahan yang efektif. Simulasi ini memberikan mahasiswa wawasan praktis yang sangat dibutuhkan dalam menjaga keamanan digital mereka, serta menumbuhkan kesadaran tentang pentingnya berhati-hati dalam setiap tindakan digital. Melalui contoh kasus nyata, mahasiswa dapat lebih memahami cara mengenali modus kejahatan dan menerapkan langkah-langkah pencegahan yang tepat.

Evaluasi dan Survei Awal-Akhir

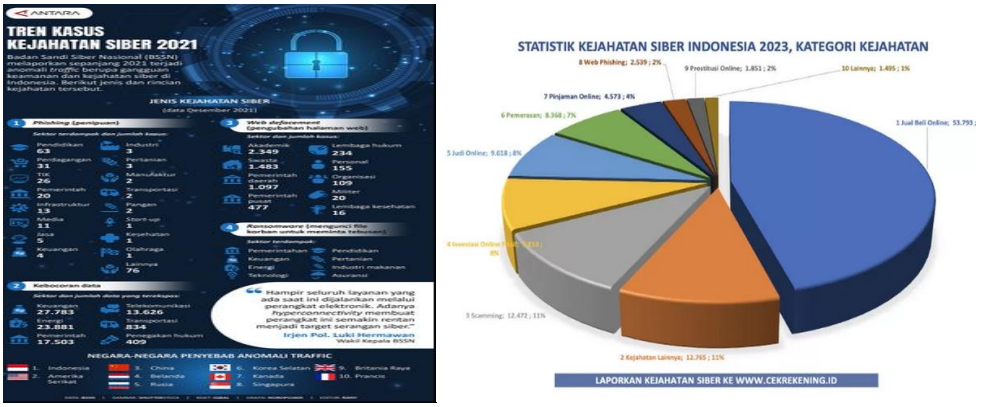
Untuk mengukur efektivitas program, dilakukan evaluasi melalui survei awal dan akhir. Survei awal dilakukan sebelum kegiatan sosialisasi dimulai, dengan tujuan menilai tingkat pemahaman awal mahasiswa tentang keamanan digital dan risiko penggunaan Dompet Digital. Survei ini mencakup pertanyaan mengenai pengetahuan dasar tentang risiko digital, pengalaman pribadi terkait keamanan Dompet Digital, serta sikap mereka terhadap pentingnya menjaga keamanan akun. Setelah kegiatan sosialisasi, workshop, dan simulasi selesai, survei akhir dilakukan untuk mengukur peningkatan pengetahuan dan perubahan sikap mahasiswa terhadap keamanan digital. Survei ini menguji pemahaman

mahasiswa terhadap konsep-konsep yang telah disampaikan, seperti tanda-tanda modus penipuan, cara menjaga akun Dompet Digital, serta perubahan dalam cara mereka menyikapi risiko digital. Survei akhir juga mencakup pertanyaan mengenai penerapan langkah-langkah keamanan dalam penggunaan Dompet Digital sehari-hari. Dengan membandingkan hasil survei awal dan akhir, efektivitas kegiatan dapat diukur secara objektif. Hasil evaluasi ini juga memberikan gambaran mengenai keberhasilan pendekatan sosialisasi dan edukasi yang diterapkan dalam program, serta memberikan masukan untuk perbaikan program pengabdian masyarakat di masa depan.

3. PEMBAHASAN

Penggunaan Dompet Digital atau dompet digital di kalangan mahasiswa Indonesia kian meningkat seiring dengan kemajuan teknologi dan peralihan gaya hidup ke arah digital. Dompet Digital memberikan kemudahan dalam berbagai transaksi, mulai dari pembelian makanan, pembayaran transportasi, hingga pembelian produk online, yang semuanya dapat dilakukan hanya dengan beberapa kali klik (Badri, 2020). Namun, di balik kemudahan tersebut, Dompet Digital juga membawa risiko keamanan yang cukup besar, terutama terkait dengan pencurian data, penipuan digital, dan serangan siber lainnya. Mahasiswa yang cenderung lebih terpapar pada teknologi sering kali menjadi sasaran utama para pelaku kejahatan digital karena mereka kerap kurang memahami pentingnya keamanan digital dalam penggunaan Dompet Digital (Afista *et al.*, 2024).

Seiring meningkatnya penggunaan Dompet Digital, ancaman terhadap keamanan digital juga semakin meningkat (Sukmawati and Kowanda, 2022). Berbagai modus serangan siber, seperti phishing, malware, dan social engineering, kini sering kali menyasar pengguna yang kurang waspada, terutama mereka yang minim pengetahuan terkait keamanan digital. Berdasarkan laporan terbaru, Indonesia mencatat jumlah serangan siber yang signifikan dalam beberapa tahun terakhir, dengan lebih dari 370 juta serangan pada tahun 2021, meskipun angka ini sedikit menurun pada tahun 2022, seperti yang digambarkan pada ilustrasi dibawah ini.



Gambar 1. Jumlah Serangan Siber

Phishing adalah salah satu metode penipuan paling umum, di mana pelaku mengirimkan pesan yang tampak berasal dari sumber tepercaya, seperti lembaga keuangan atau penyedia layanan Dompet Digital, untuk meminta informasi sensitif pengguna, seperti kata sandi atau nomor PIN. Pesan tersebut biasanya berisi tautan palsu yang mengarahkan pengguna ke situs web yang meniru tampilan situs resmi, dan ketika pengguna memasukkan data mereka, informasi tersebut jatuh ke tangan pelaku (Sukmawati and Kowanda, 2022).

Selain phishing, malware atau perangkat lunak berbahaya juga menjadi ancaman signifikan bagi pengguna Dompet Digital. Malware dapat disebarkan melalui unduhan aplikasi yang tidak resmi atau situs web yang mencurigakan. Setelah malware berhasil masuk ke perangkat pengguna, perangkat lunak ini dapat merekam aktivitas pengguna, mencuri kata sandi, dan mengakses data pribadi lainnya tanpa sepengetahuan mereka. Kemudian, ada risiko kebocoran data, di mana data pengguna Dompet Digital, seperti riwayat transaksi dan informasi akun, mungkin bocor akibat serangan pada penyedia layanan atau karena pengguna kurang berhati-hati dalam menjaga keamanan akun mereka (Prameswari *et al.*, 2022).

Untuk melindungi diri dari risiko-risiko tersebut, pengguna Dompet Digital, terutama mahasiswa, harus memahami prinsip-prinsip dasar keamanan digital. Salah satu langkah pertama yang harus dilakukan adalah menggunakan autentikasi dua faktor (2FA). Fitur 2FA menambahkan lapisan keamanan ekstra pada akun Dompet Digital dengan meminta verifikasi tambahan selain kata sandi. Biasanya, verifikasi ini dilakukan melalui kode OTP (One-Time Password) yang dikirimkan ke nomor telepon atau email pengguna. Dengan demikian, meskipun seseorang berhasil mendapatkan kata sandi pengguna, mereka tetap tidak dapat mengakses akun tanpa kode verifikasi tersebut (Widjojo, 2020).

Menurut Sukmawati and Kowanda, (2022) kata sandi yang kuat juga sangat penting untuk keamanan akun. Pengguna sebaiknya menghindari penggunaan kata sandi yang

mudah ditebak, seperti tanggal lahir atau nama panggilan, dan menggunakan kombinasi karakter yang unik. Pengguna juga dianjurkan untuk mengganti kata sandi secara berkala dan tidak menggunakan kata sandi yang sama untuk berbagai akun, guna mengurangi risiko jika salah satu akun mengalami kebocoran data.

Selanjutnya, salah satu cara paling efektif untuk menjaga keamanan dalam penggunaan Dompet Digital adalah dengan rutin memverifikasi transaksi dan memeriksa riwayat transaksi. Langkah ini membantu pengguna untuk segera mengenali aktivitas mencurigakan atau transaksi yang tidak dilakukan, sehingga dapat segera melapor dan mengambil tindakan pencegahan (Antoni, 2023). Selain itu, penggunaan metode verifikasi tambahan seperti One-Time Password (OTP) dalam setiap transaksi juga sangat penting untuk memastikan bahwa setiap transaksi dilakukan oleh pemilik akun yang sah.

Mahasiswa juga disarankan untuk menghindari berbagi informasi pribadi dan detail keuangan di media sosial atau platform online lainnya yang tidak aman. Kebiasaan berbagi data secara sembarangan di dunia maya bisa menjadi pintu masuk bagi pelaku kejahatan untuk mengeksploitasi informasi tersebut. Hal ini termasuk berbagi informasi mengenai kartu identitas, nomor telepon, atau informasi keuangan di platform yang tidak tepercaya.

Selain itu, mahasiswa harus memastikan bahwa aplikasi Dompet Digital yang mereka gunakan diunduh dari sumber resmi, seperti Google Play Store atau App Store (Afista *et al.*, 2024). Mengunduh aplikasi dari sumber yang tidak resmi dapat meningkatkan risiko terkena malware atau aplikasi palsu yang dirancang untuk mencuri data pengguna. Mereka juga harus memperbarui aplikasi Dompet Digital secara berkala, karena setiap pembaruan biasanya mencakup perbaikan fitur keamanan untuk melindungi pengguna dari ancaman yang terus berkembang.

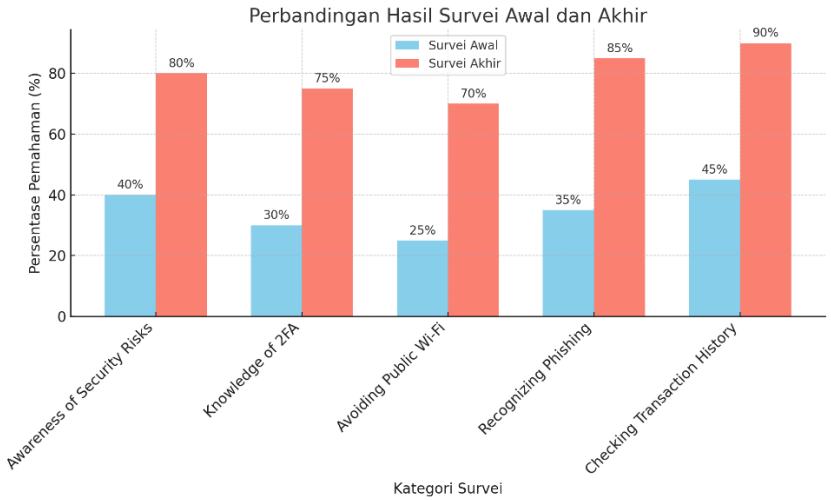
Penyedia Dompet Digital memiliki tanggung jawab besar dalam menjaga keamanan data dan transaksi pengguna. Untuk itu, banyak penyedia layanan Dompet Digital yang telah menyediakan berbagai fitur keamanan, seperti autentikasi dua faktor (2FA), enkripsi data, pemindaian biometrik, serta pemantauan transaksi. Fitur-fitur ini dirancang untuk melindungi pengguna dari berbagai risiko keamanan digital, seperti pencurian data dan transaksi tidak sah. Tabel berikut memberikan perbandingan fitur keamanan dari beberapa Dompet Digital terkemuka di Indonesia. Informasi ini membantu pengguna memahami fitur keamanan spesifik yang ditawarkan oleh masing-masing platform dan dapat menjadi panduan dalam memilih Dompet Digital yang paling sesuai dengan kebutuhan dan preferensi keamanan mereka.

Tabel 1. Perbandingan Fitur Keamanan Dompet Digital di Indonesia

Fitur keamanan	**GoPay**	**OVO**	**DANA**	**LinkAja**	**ShopeePay**
Autentikasi Dua Faktor (2FA)	Ya	Ya	Ya	Ya	Ya
Enkripsi Data	Ya	Ya	Ya	Ya	Ya
Pemindaian Sidik Jari/Wajah	Ya	Ya	Ya	Tidak	Ya
Pemantauan Transaksi	Ya	Ya	Ya	Ya	Ya
Jaminan Uang Kembali	Tidak	Tidak	Ya	Tidak	Tidak
Notifikasi Real-Time	Ya	Ya	Ya	Ya	Ya

Hasil survei menunjukkan adanya peningkatan yang signifikan dalam pemahaman mahasiswa mengenai keamanan digital setelah mengikuti program edukasi ini. Peningkatan pemahaman ini terlihat pada berbagai kategori, mulai dari kesadaran akan risiko keamanan, pemahaman tentang autentikasi dua faktor (2FA), hingga kemampuan mengenali modus phishing. Sebelum program dilaksanakan, rata-rata pemahaman mahasiswa di setiap kategori berada pada tingkat yang rendah, dengan persentase pemahaman awal berkisar antara 25% hingga 45%. Namun, setelah mengikuti program, persentase pemahaman mahasiswa di setiap kategori meningkat tajam, dengan angka rata-rata antara 70% hingga 90%.

Grafik berikut ini menggambarkan perbandingan hasil survei awal dan akhir, menunjukkan perbedaan yang signifikan dalam pemahaman mahasiswa sebelum dan setelah program edukasi. Dengan adanya peningkatan ini, dapat disimpulkan bahwa program edukasi dan workshop yang diadakan berhasil meningkatkan literasi keamanan digital mahasiswa, serta membekali mereka dengan keterampilan praktis untuk mengamankan akun Dompet Digital mereka.



Gambar 2. Perbandingan Hasil Survei Awal Dan Akhir

Dengan keterlibatan aktif mahasiswa dalam menyebarkan informasi ini, diharapkan terbentuk komunitas kampus yang lebih sadar akan pentingnya keamanan digital. Mahasiswa dapat saling mengingatkan dan berbagi informasi tentang ancaman terbaru serta cara-cara menghindarinya, sehingga keamanan digital menjadi bagian yang tidak terpisahkan dari kehidupan sehari-hari mereka. Edukasi ini juga diharapkan mampu menciptakan generasi muda yang lebih siap menghadapi tantangan keamanan digital di masa depan, yang semakin kompleks seiring dengan perkembangan teknologi.

4. KESIMPULAN DAN REKOMENDASI

Kesimpulan

Dalam era digital yang serba cepat dan terintegrasi, literasi keamanan digital menjadi sangat penting, khususnya dalam penggunaan Dompet Digital di kalangan mahasiswa. Program pengabdian masyarakat ini menekankan betapa pentingnya pemahaman yang mendalam akan risiko-risiko digital seperti phishing, malware, dan pencurian data, serta memberikan wawasan tentang langkah-langkah dasar keamanan yang dapat diambil oleh pengguna untuk melindungi akun dan data pribadi mereka. Kesadaran mahasiswa akan risiko ini, diiringi dengan kemampuan praktis dalam menerapkan keamanan digital, dapat mencegah mereka menjadi korban dari kejahatan siber yang semakin marak.

Harapan besar dari program ini adalah agar mahasiswa tidak hanya melindungi diri mereka sendiri, tetapi juga menjadi agen perubahan yang aktif dalam menyebarkan pengetahuan ini kepada sesama. Dengan semakin banyak mahasiswa yang paham dan waspada terhadap ancaman keamanan digital, ekosistem kampus yang lebih aman secara digital dapat terbentuk. Mahasiswa yang memiliki kesadaran tinggi dan pengetahuan yang

baik mengenai keamanan Dompet Digital diharapkan dapat mengedukasi teman-teman mereka, menciptakan komunitas yang saling peduli dan waspada terhadap risiko-risiko yang mungkin timbul dalam penggunaan teknologi keuangan.

Rekomendasi

Sebagai tindak lanjut, penting untuk mempertimbangkan edukasi rutin mengenai keamanan digital, baik yang diadakan secara langsung di kampus maupun melalui media online. Kegiatan edukasi berkelanjutan ini dapat berupa seminar, webinar, atau lokakarya yang melibatkan mahasiswa secara aktif, agar mereka selalu diperbarui dengan ancaman digital terbaru serta cara-cara yang efektif untuk melindungi diri. Selain itu, untuk memperkuat pesan-pesan keamanan, kampus juga bisa mempertimbangkan menyebarkan konten edukatif melalui media sosial, yang mudah diakses mahasiswa sehari-hari.

Kolaborasi dengan penyedia layanan Dompet Digital merupakan langkah strategis untuk mengembangkan kegiatan edukatif serupa secara berkala. Penyedia layanan Dompet Digital biasanya memiliki keahlian dan sumber daya untuk mendukung pelatihan keamanan digital dengan informasi yang terkini. Dengan bekerja sama dengan kampus, mereka dapat membantu mengadakan kegiatan sosialisasi yang tidak hanya mencakup mahasiswa, tetapi juga pengguna Dompet Digital lainnya. Kolaborasi ini diharapkan mampu menciptakan lingkungan digital yang lebih aman secara menyeluruh, serta mengurangi risiko kejahatan digital yang mengancam pengguna Dompet Digital. Dengan langkah-langkah ini, diharapkan keamanan digital akan semakin tertanam dalam kehidupan sehari-hari mahasiswa dan masyarakat pada umumnya.

DAFTAR REFERENSI

Afista, T.L. et al. (2024) ‘Analisis perilaku konsumtif gen-z terhadap digital e-wallet DANA’, Jurnal Pendidikan Tambusai, 8(1), pp. 3344–3350.

Antoni, S. (2023) ‘Factors Influencing Interest in Using Dana and Ovo E-Wallets in the Millennial Generation’, Ekspansi: Jurnal Ekonomi, Keuangan, Perbankan, Dan Akuntansi, 15(2), pp. 118–131.

Badri, M. (2020) ‘Adopsi inovasi aplikasi dompet digital di Kota Pekanbaru’, Inovbiz: Jurnal Inovasi Bisnis, 8(1), pp. 120–127.

Gunawan, A.A.L. and Winarti, A. (2022) ‘Pengaruh aplikasi dompet digital terhadap transaksi dimasa kini’, Nautical: Jurnal Ilmiah Multidisiplin Indonesia, 1(6), pp. 352–356.

Hartono, M.B. (2023) ‘Pengaruh Persepsi Kegunaan Dan Persepsi Risiko Terhadap Minat Menggunakan Berkelanjutan Yang Di Mediasi Oleh Sikap Penggunaan Pada Aplikasi

Dompet Digital Ovo Dan Dana (Studi Komparasi Di Kota Pontianak)', Jurnal Ekonomi Dan Manajemen, 2(2), pp. 11–22.

Herdioko, J. (2023) 'Analisis Motivasi Penggunaan Dompet Digital Dana pada Masyarakat di Daerah Istimewa Yogyakarta', in Prosiding Seminar Nasional Forum Manajemen Indonesia-e-ISSN 3026-4499, pp. 38–54.

Inaya, C., Ismiarti, R.J. and Nofirda, F.A. (2024) 'Analisis Dampak Penggunaan Dompet Digital pada Generasi Milenial: Studi Komparasi Gopay dan Ovo/Dana', Jurnal Pendidikan Tambusai, 8(1), pp. 3159–3164.

Prameswari, A. et al. (2022) 'Analisis Faktor-Faktor Yang Mempengaruhi Minat Mahasiswa UINSU Medan Dalam Menggunakan Sistem Pembayaran E-Wallet', JUSIBI (Jurnal Sistem Informasi dan Bisnis), 4(1), pp. 60–70.

Sukmawati, K. and Kowanda, D. (2022) 'Keputusan Penggunaan E-Wallet Gopay Berdasarkan Pengaruh Keamanan, Persepsi Kemudahan Dan Persepsi Manfaat', Jurnal Ilmiah Multidisiplin, 1(05), pp. 66–72.

Widjojo, R. (2020) 'The development of digital payment systems in Indonesia: a review of go-pay and ovo e-wallets', Economic Alternatives, 3, pp. 384–395.