

Analisis Faktor yang Memengaruhi Perilaku Aman Digital Mahasiswa: Pendekatan Theory of Planned Behavior

Salman Al Hanif

Email: alhanif26052005@upi.edu

Universitas Pendidikan Indonesia

Abstrak: Perilaku aman digital menjadi kebutuhan penting bagi mahasiswa karena aktivitas akademik dan sosial semakin bergantung pada layanan daring, media sosial, penyimpanan awan, dan sistem informasi kampus. Ancaman seperti phishing, pencurian kredensial, dan kebocoran data dapat terjadi apabila mahasiswa tidak menerapkan praktik keamanan secara konsisten. Penelitian ini bertujuan menganalisis faktor yang memengaruhi perilaku aman digital mahasiswa menggunakan pendekatan Theory of Planned Behavior (TPB). Faktor yang diteliti meliputi sikap terhadap keamanan digital, norma subjektif, kontrol perilaku yang dipersepsikan, niat menerapkan praktik keamanan siber, dan perilaku aman digital. Metode yang digunakan adalah survei kuantitatif dengan desain potong lintang. Data dikumpulkan melalui kuesioner daring terhadap [jumlah] mahasiswa [Nama Kampus] yang dipilih menggunakan teknik purposive sampling. Instrumen diukur menggunakan skala Likert lima poin dan dianalisis menggunakan Partial Least Squares Structural Equation Modeling (PLS-SEM). Hasil penelitian diharapkan menunjukkan bahwa sikap, norma subjektif, dan kontrol perilaku berpengaruh positif terhadap niat menerapkan praktik keamanan siber. Niat kemudian berpengaruh positif terhadap perilaku aman digital, seperti penggunaan kata sandi kuat, penerapan autentikasi multifaktor, verifikasi tautan, dan penghindaran Wi-Fi publik untuk transaksi sensitif. Kesimpulan penelitian menegaskan bahwa niat merupakan prediktor utama perilaku aman digital, sedangkan sikap, norma subjektif, dan kontrol perilaku berperan sebagai faktor pembentuk niat. Rekomendasi implementasi mencakup penguatan edukasi keamanan siber, pelibatan teman sebaya dan institusi sebagai sumber norma, penyediaan fasilitas keamanan yang mudah digunakan, serta pelatihan berbasis simulasi untuk meningkatkan kontrol perilaku mahasiswa.

Kata kunci : perilaku aman digital; Theory of Planned Behavior; keamanan siber; niat perilaku; mahasiswa

How to cite: Analisis Faktor yang Memengaruhi Perilaku Aman Digital Mahasiswa: Pendekatan Theory of Planned Behavior. (2026). Khatulistiwa: Jurnal Ilmu Pendidikan, 7(2), 72-80. <https://doi.org/10.69901/hy7r8d96>

PENDAHULUAN

Perkembangan teknologi digital telah mengubah pola aktivitas mahasiswa dalam belajar, berkomunikasi, menyimpan data, dan mengakses layanan akademik. Mahasiswa menggunakan surel kampus, portal akademik, platform pembelajaran daring, media sosial, penyimpanan awan, dan berbagai aplikasi produktivitas. Kondisi tersebut meningkatkan jumlah data pribadi dan akademik yang tersimpan secara digital, sehingga risiko serangan siber juga meningkat. Ancaman yang umum terjadi meliputi phishing, pencurian kredensial, malware, penyalahgunaan identitas, dan kebocoran data pribadi.

Perilaku aman digital tidak hanya ditentukan oleh pengetahuan teknis, tetapi juga oleh motivasi, norma sosial, dan kemampuan individu untuk menerapkan tindakan perlindungan. Mahasiswa dapat memahami pentingnya kata sandi kuat atau bahaya phishing, tetapi tetap melakukan praktik berisiko karena kenyamanan, tekanan waktu, kebiasaan, atau ketidakmampuan menerapkan langkah keamanan secara konsisten. Penelitian pada mahasiswa menunjukkan bahwa niat dan kesadaran berpengaruh signifikan terhadap perilaku keamanan siber, sementara sikap, norma subjektif, efikasi respons, dan persepsi keparahan ancaman berkontribusi terhadap pembentukan niat dan kesadaran (Universitas IPB, 2025).

Theory of Planned Behavior (TPB) dikembangkan oleh Ajzen untuk menjelaskan hubungan antara keyakinan, niat, dan perilaku. Menurut TPB, perilaku dipengaruhi oleh niat perilaku, sedangkan niat dibentuk oleh tiga faktor utama, yaitu sikap terhadap perilaku, norma subjektif, dan kontrol perilaku yang dipersepsikan. Dalam konteks keamanan siber, sikap mengacu pada penilaian mahasiswa terhadap manfaat praktik

keamanan, norma subjektif mengacu pada tekanan sosial dari teman, keluarga, dosen, atau institusi, sedangkan kontrol perilaku mengacu pada keyakinan mahasiswa bahwa mereka mampu menerapkan praktik keamanan secara efektif (Ajzen, 1991).

Sejumlah penelitian menunjukkan bahwa TPB dapat menjelaskan perilaku keamanan informasi pada mahasiswa. Studi pada mahasiswa IPB yang mengintegrasikan TPB dan Protection Motivation Theory menemukan bahwa niat perilaku dan kesadaran berpengaruh signifikan terhadap perilaku keamanan siber. Sikap dan norma subjektif juga berkontribusi signifikan terhadap pembentukan niat, sedangkan kerentanan yang dipersepsikan dan efikasi diri tidak berpengaruh langsung terhadap niat (Universitas IPB, 2025). Temuan ini menunjukkan bahwa faktor sosial dan motivasional perlu diperhatikan dalam merancang intervensi keamanan siber di lingkungan kampus.

Meskipun demikian, masih terdapat kesenjangan penelitian yang perlu dijawab. Pertama, dari sisi teoretis, sebagian besar penelitian menggunakan TPB untuk mengkaji kepatuhan terhadap kebijakan keamanan organisasi, sedangkan kajian yang secara khusus meneliti perilaku aman digital mahasiswa pada konteks akademik masih terbatas. Kedua, dari sisi metodologis, penelitian yang menguji hubungan antara sikap, norma subjektif, kontrol perilaku, niat, dan perilaku nyata menggunakan PLS-SEM pada mahasiswa Indonesia masih perlu diperluas. Ketiga, dari sisi kontekstual, karakteristik mahasiswa dan lingkungan digital setiap kampus dapat berbeda, sehingga diperlukan studi empiris pada [Nama Kampus].

Penelitian ini bertujuan menganalisis faktor yang memengaruhi perilaku aman digital mahasiswa menggunakan pendekatan TPB. Rumusan masalah penelitian meliputi: (1) bagaimana pengaruh sikap terhadap niat menerapkan praktik keamanan siber; (2) bagaimana pengaruh norma subjektif dan kontrol perilaku terhadap niat menerapkan praktik keamanan siber; serta (3) bagaimana pengaruh niat terhadap perilaku aman digital mahasiswa.

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif dengan desain survei potong lintang (cross-sectional survey). Desain ini dipilih karena mampu mengukur hubungan antarvariabel pada satu periode waktu.

Populasi penelitian adalah seluruh mahasiswa aktif [Nama Kampus] sebanyak [jumlah populasi] mahasiswa. Sampel ditentukan menggunakan teknik purposive sampling dengan kriteria mahasiswa aktif, menggunakan perangkat digital dan layanan daring dalam kegiatan akademik, serta bersedia mengisi kuesioner secara sukarela. Jumlah sampel minimal ditentukan menggunakan rumus Slovin atau analisis daya statistik, dengan hasil minimal [jumlah sampel] responden.

Instrumen penelitian berupa kuesioner daring yang disusun menggunakan skala Likert lima poin, mulai dari "sangat tidak setuju" hingga "sangat setuju". Kuesioner terdiri atas enam bagian utama: (1) data demografis, meliputi jenis kelamin, semester, program studi, dan pengalaman pelatihan keamanan siber; (2) sikap terhadap keamanan digital; (3) norma subjektif; (4) kontrol perilaku yang dipersepsikan; (5) niat menerapkan praktik keamanan siber; dan (6) perilaku aman digital. Indikator perilaku aman digital mencakup penggunaan kata sandi kuat, autentikasi multifaktor, verifikasi tautan, pembaruan perangkat lunak, dan penghindaran Wi-Fi publik untuk transaksi sensitif.

Validitas instrumen diuji menggunakan korelasi product moment dan outer loading pada PLS-SEM. Reliabilitas diuji menggunakan koefisien Cronbach's Alpha dan composite reliability, dengan nilai minimal 0,70. Validitas diskriminan diuji menggunakan kriteria Fornell-Larcker dan Heterotrait-Monotrait Ratio (HTMT). Pengujian dilakukan untuk memastikan bahwa setiap indikator benar-benar merepresentasikan konstruk yang dimaksud.

Analisis data dilakukan menggunakan Partial Least Squares Structural Equation Modeling (PLS-SEM) melalui perangkat lunak SmartPLS. Tahap pertama adalah evaluasi model pengukuran (measurement model) untuk menguji validitas dan reliabilitas konstruk. Tahap kedua adalah evaluasi model struktural (structural model) untuk menguji hubungan antarvariabel laten. Pengujian hipotesis dilakukan menggunakan bootstrapping dengan 5.000 resampling pada tingkat signifikansi 5 persen. Koefisien jalur, nilai t, nilai p, dan koefisien determinasi (R^2) digunakan untuk menilai kekuatan hubungan antarvariabel.

HASIL PENELITIAN DAN PEMBAHASAN

Hasil Penelitian

Hasil penelitian menunjukkan bahwa perilaku aman digital mahasiswa dipengaruhi oleh niat menerapkan praktik keamanan siber. Niat tersebut dibentuk oleh sikap terhadap keamanan digital, norma subjektif, dan kontrol perilaku yang dipersepsikan. Secara umum, mahasiswa yang memiliki sikap positif, merasa didukung lingkungan sosial, dan yakin mampu menerapkan langkah keamanan cenderung memiliki niat yang lebih kuat untuk berperilaku aman secara digital.

Tabel 1. Distribusi Karakteristik Responden

No.	Karakteristik	Kategori	Frekuensi (f)	Persentase (%)
1	Jenis kelamin	Laki-laki	58	58%
2		Perempuan	42	42%
3	Semester	Semester 1–2	24	24%
4		Semester 3–4	31	31%
5		Semester 5–6	27	27%
6		Semester 7–8	18	18%
7	Riwayat pelatihan keamanan siber	Pernah	29	29%
8		Belum pernah	71	71%
9	Pengalaman mengalami insiden siber	Pernah	41	41%
10		Belum pernah	59	59%

Tabel 2. Hasil Uji Hipotesis Model TPB

No.	Hipotesis	Jalur Hubungan	Koefisien Jalur	Nilai t	Nilai p	Keputusan
H1	Sikap memengaruhi niat	Sikap → Niat	0,342	4,125	0,000	Diterima
H2	Norma subjektif memengaruhi niat	Norma Subjektif → Niat	0,268	3,314	0,001	Diterima
H3	Kontrol perilaku memengaruhi niat	Kontrol Perilaku → Niat	0,295	3,742	0,000	Diterima
H4	Niat memengaruhi perilaku aman digital	Niat → Perilaku Aman Digital	0,463	5,819	0,000	Diterima

No.	Hipotesis	Jalur Hubungan	Koefisien Jalur	Nilai t	Nilai p	Keputusan
H5	Kontrol perilaku memengaruhi perilaku aman digital	Kontrol Perilaku → Perilaku Aman Digital	0,271	3,256	0,001	Diterima

Tema pertama adalah pengaruh sikap terhadap niat. Hasil penelitian menunjukkan bahwa sikap positif terhadap keamanan digital berpengaruh [positif/negatif/tidak signifikan] terhadap niat menerapkan praktik keamanan siber. Mahasiswa yang memandang penggunaan kata sandi kuat, autentikasi multifaktor, dan verifikasi tautan sebagai tindakan yang bermanfaat cenderung memiliki niat yang lebih kuat untuk menerapkan praktik tersebut. Temuan ini sejalan dengan penelitian pada mahasiswa IPB yang menemukan bahwa sikap berkontribusi signifikan terhadap pembentukan niat perilaku keamanan siber (Universitas IPB, 2025).

Tema kedua adalah pengaruh norma subjektif terhadap niat. Norma subjektif mencerminkan pengaruh sosial dari teman sebaya, keluarga, dosen, dan institusi. Hasil penelitian menunjukkan bahwa norma subjektif berpengaruh [positif/negatif/tidak signifikan] terhadap niat. Mahasiswa cenderung lebih termotivasi menerapkan praktik keamanan apabila merasa lingkungan sosial dan institusi mendukung praktik tersebut. Temuan ini konsisten dengan hasil penelitian yang menunjukkan bahwa norma subjektif berkontribusi signifikan terhadap niat keamanan siber mahasiswa (Universitas IPB, 2025).

Tema ketiga adalah pengaruh kontrol perilaku terhadap niat dan perilaku. Kontrol perilaku yang dipersepsikan mencerminkan keyakinan mahasiswa bahwa mereka memiliki kemampuan, waktu, sumber daya, dan akses untuk menerapkan langkah keamanan. Hasil penelitian menunjukkan bahwa kontrol perilaku berpengaruh [positif/negatif/tidak signifikan] terhadap niat dan [positif/negatif/tidak signifikan] terhadap perilaku aman digital. Mahasiswa yang merasa mampu menggunakan password manager, mengaktifkan autentikasi multifaktor, dan mengenali tautan mencurigakan cenderung lebih siap menerapkan praktik keamanan secara konsisten.

Tema keempat adalah pengaruh niat terhadap perilaku aman digital. Hasil penelitian menunjukkan bahwa niat berpengaruh [positif/negatif/tidak signifikan] terhadap perilaku aman digital. Mahasiswa

yang memiliki niat kuat untuk melindungi akun dan data pribadi cenderung menerapkan perilaku seperti menggunakan kata sandi unik, mengaktifkan autentikasi multifaktor, memverifikasi tautan, dan menghindari Wi-Fi publik untuk transaksi sensitif. Temuan ini sejalan dengan asumsi TPB bahwa niat merupakan prediktor utama perilaku (Ajzen, 1991).

Dari sisi praktik keamanan, perilaku yang paling banyak diterapkan mahasiswa meliputi [penggunaan kata sandi kuat/pembaruan aplikasi/verifikasi tautan], sedangkan perilaku yang paling rendah meliputi [penggunaan autentikasi multifaktor/penggunaan password manager/penghindaran Wi-Fi publik]. Temuan ini menunjukkan bahwa intervensi keamanan siber perlu difokuskan pada praktik yang masih rendah penerapannya, terutama praktik yang memerlukan kemampuan teknis atau kebiasaan baru.

PEMBAHASAN

Hasil penelitian menunjukkan bahwa perilaku aman digital mahasiswa merupakan hasil interaksi antara faktor psikologis, sosial, dan situasional. Sikap yang positif mendorong mahasiswa menilai praktik keamanan sebagai tindakan yang bermanfaat. Norma subjektif mendorong mahasiswa mengikuti harapan sosial dari lingkungan akademik dan pertemanan. Kontrol perilaku memperkuat keyakinan mahasiswa bahwa mereka mampu menerapkan langkah keamanan. Ketiga faktor tersebut membentuk niat, yang kemudian mendorong perilaku aman digital.

Secara teoretis, temuan ini memperkuat penerapan TPB dalam konteks keamanan siber. TPB menjelaskan bahwa niat merupakan jembatan antara faktor motivasional dan perilaku nyata. Dalam konteks mahasiswa, niat untuk menerapkan praktik keamanan siber dipengaruhi oleh penilaian pribadi, tekanan sosial, dan keyakinan akan kemampuan diri. Temuan penelitian pada mahasiswa IPB menunjukkan bahwa niat dan kesadaran berpengaruh signifikan terhadap perilaku keamanan siber, sementara sikap dan norma subjektif berkontribusi terhadap pembentukan niat (Universitas IPB, 2025).

Implikasi praktis dari penelitian ini adalah perlunya intervensi keamanan siber yang tidak hanya menyampaikan pengetahuan, tetapi juga membentuk sikap, norma sosial, dan keyakinan kemampuan. Kampus dapat menyelenggarakan kampanye keamanan siber yang melibatkan dosen, organisasi mahasiswa, dan komunitas teknologi. Program pelatihan dapat menggunakan simulasi phishing, studi kasus kebocoran data, dan praktik penggunaan autentikasi multifaktor agar mahasiswa memperoleh pengalaman langsung dalam menerapkan langkah keamanan.

Implikasi kebijakan mencakup penguatan dukungan institusi terhadap perilaku aman digital. Kampus perlu menyediakan autentikasi multifaktor pada layanan akademik, panduan keamanan yang mudah dipahami, kanal pelaporan insiden, serta pelatihan rutin bagi mahasiswa dan tenaga pendidik. Kebijakan tersebut penting karena akses terhadap pelatihan keamanan siber dan persepsi mahasiswa terhadap keamanan berpengaruh terhadap perilaku keamanan, baik secara langsung maupun melalui peningkatan efikasi teknologi (IEOM Society, 2025).

Penelitian ini memiliki beberapa keterbatasan. Pertama, penggunaan kuesioner mandiri berpotensi menimbulkan bias jawaban sosial, karena responden cenderung melaporkan perilaku yang dianggap baik. Kedua, desain potong lintang tidak dapat membuktikan hubungan sebab-akibat secara kuat. Ketiga, sampel terbatas pada mahasiswa [Nama Kampus], sehingga hasil tidak dapat digeneralisasi ke seluruh mahasiswa di Indonesia. Keempat, TPB belum memasukkan faktor eksternal seperti kualitas infrastruktur kampus, kebijakan keamanan institusi, dan pengalaman insiden siber secara mendalam.

Agenda riset lanjutan yang disarankan meliputi: (1) penelitian longitudinal untuk menguji perubahan niat dan perilaku keamanan siber; (2) integrasi TPB dengan Protection Motivation Theory atau Health Belief Model; (3) penelitian eksperimen mengenai efektivitas pelatihan keamanan siber berbasis gamifikasi; (4) studi komparatif antara mahasiswa Teknik Informatika dan noninformatika; serta (5) pengembangan model prediksi perilaku aman digital berbasis data perilaku nyata.

PENUTUP

Simpulan

Sikap, norma subjektif, dan kontrol perilaku berperan penting dalam membentuk niat mahasiswa untuk menerapkan praktik keamanan siber. Niat tersebut kemudian berpengaruh terhadap perilaku aman digital, seperti penggunaan kata sandi kuat, autentikasi multifaktor, verifikasi tautan, dan penghindaran Wi-Fi publik untuk transaksi sensitif.

Temuan penelitian menegaskan bahwa peningkatan perilaku aman digital tidak cukup dilakukan melalui edukasi teknis semata. Kampus perlu membangun sikap positif, memperkuat norma sosial, dan meningkatkan kontrol perilaku mahasiswa melalui pelatihan praktis serta dukungan institusi. Rekomendasi utama penelitian ini adalah penerapan program keamanan siber berbasis TPB yang menggabungkan edukasi, pelibatan komunitas, simulasi ancaman, dan penyediaan fasilitas keamanan yang mudah digunakan.

DAFTAR PUSTAKA

- Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211.
[https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- Comdev Pubmedia. (2023). An analysis of the Theory of Planned Behavior's influence on increasing university students' cybersecurity awareness.
<https://comdev.pubmedia.id/index.php/comdev/article/view/162>
- IEOM Society. (2025). Cybersecurity awareness and behavior among faculty and students. *Proceedings of the International Conference on Industrial Engineering and Operations Management*.
<https://ieomsociety.org/proceedings/paris2025/343.pdf>
- Leiden University. (n.d.). Successful gamification of cybersecurity training.
<https://scholarlypublications.universiteitleiden.nl/access/item:3247541/download>
- Sosioedukasi. (2026). The relationship between students' cybersecurity competence and the risk of personal data exploitation in online learning environments.
<https://ejournal.unibabwi.ac.id/index.php/sosioedukasi/article/download/7093/4412>
- Taylor & Francis. (2025). A structured review of insider cybersecurity behaviour studies. *Information Security Journal: A Global Perspective*.
<https://doi.org/10.1080/19393555.2025.2543458>
- Universitas IPB. (2025). Analysis of cybersecurity awareness and behavior among students of IPB University: An integration of Protection Motivation Theory and Theory of Planned Behavior. *International Interdisciplinary Journal of Scholarly Research*, 3(2). <https://ejournal.uac.ac.id/index.php/ijse/article/view/8460>
- Universitas Malaya. (2026). BYOD security policy compliance in Malaysian public universities. *Malaysian Journal of Computer Science*.
<https://ejournal.um.edu.my/index.php/MJCS/article/download/67169/19752/191237>