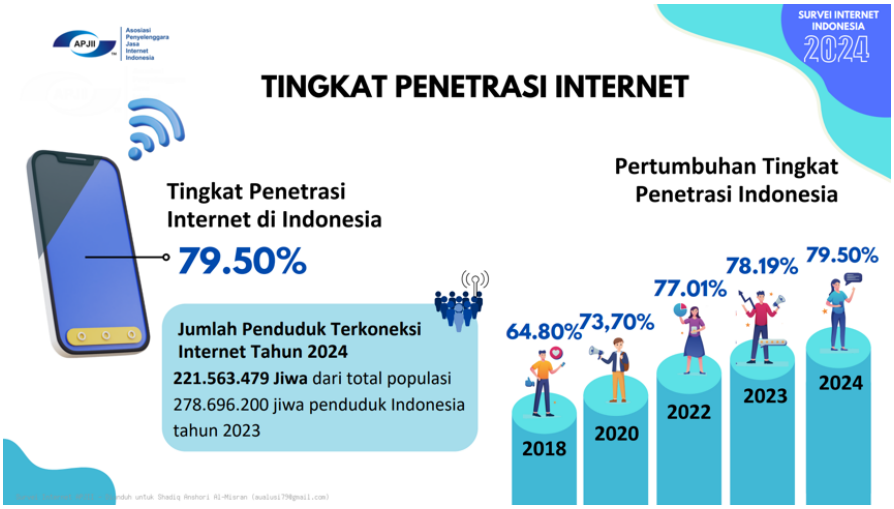
BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Masyarakat Indonesia telah mengadopsi teknologi digital secara masif dalam kehidupan sehari-hari. Kemudahan berbagi dan menemukan informasi pribadi melalui media sosial atau pencarian daring telah meningkat, tetapi tanpa kesadaran keamanan siber yang memadai, pengguna mungkin menghadapi tantangan dalam menentukan apakah akan mengungkapkan data mereka (Alrobaian et al., 2023). Tingginya tingkat penetrasi internet menunjukkan bahwa teknologi digital telah menjadi bagian tak terpisahkan dari kehidupan masyarakat Indonesia. Namun, tingginya penetrasi internet ini tidak selalu diiringi dengan kesadaran keamanan digital yang memadai.

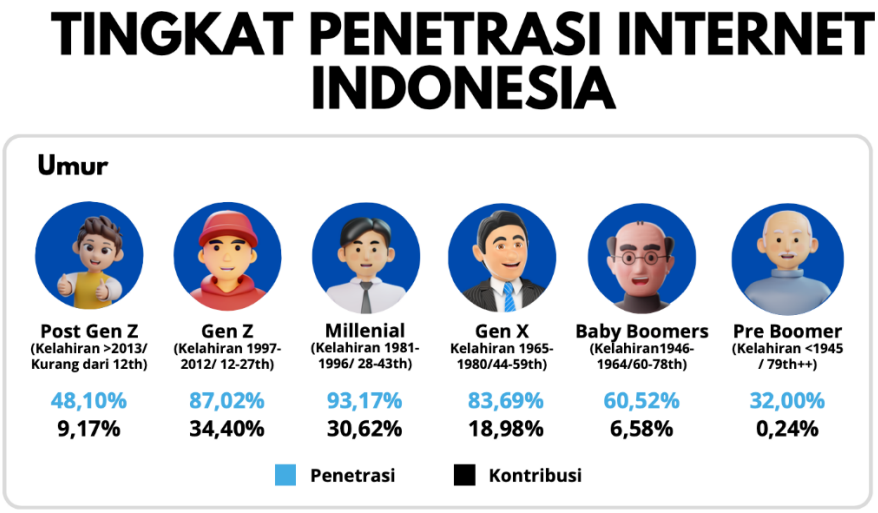


Gambar 1.1 Tingkat Penetrasi Internet di Indonesia

Sumber : Asosiasi Penyelenggara Jasa Internet Indonesia (2024)

Dari gambar diatas dapat dilihat bahwa Tingkat penetrasi Indonesia sudah mencapai 79,50%. Berdasarkan survey yang dilakukan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), menunjukkan bahwa sebanyak 221.563.479 jiwa dari 278.696.200 jiwa pada tahun 2023 masyarakat Indonesia telah terhubung ke internet. Hal ini memberikan Gambaran bahwa konektivitas internet di Indonesia sudah semakin luas dan pesat. Pertumbuhan ini menunjukkan

bahwa internet semakin penting dalam kehidupan Namun, tingkat penggunaan internet ini berbeda antara generasi yang lebih muda dan generasi yang lebih tua. Perbedaan ini terlihat jelas ketika dilihat dari pola penggunaan teknologi antar generasi.



Gambar 1.2 Tingkat Penetrasi Internet Tiap Generasi di Indonesia

Sumber : Asosiasi Penyelenggara Jasa Internet Indonesia (2024)

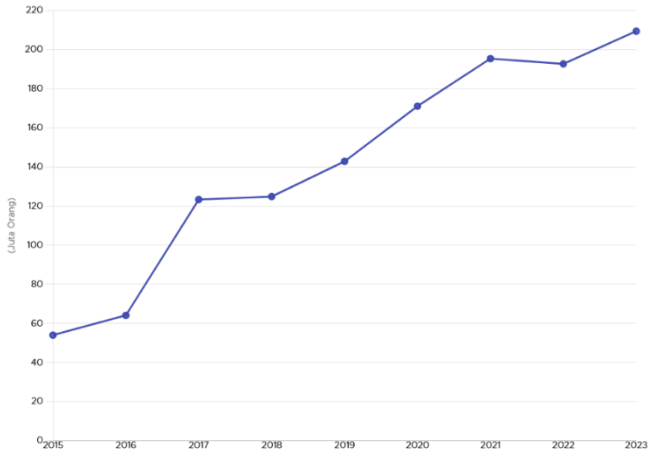
Generasi Milenial dan Gen Z merupakan kelompok pengguna internet terbesar di Indonesia, menyumbang lebih dari 65% dari total pengguna internet, sementara generasi Baby Boomers dan Pre Boomers menunjukkan tingkat adopsi teknologi yang lebih rendah. Meskipun generasi muda memiliki tingkat keterpaparan teknologi yang lebih tinggi, kesadaran keamanan siber *(cybersecurity awareness)* mereka tidak selalu optimal. Faktor seperti pengetahuan keamanan siber (*cybersecurity knowledge*), kebiasaan dalam mengelola kata sandi (password security), pemahaman terhadap keamanan email (email security), dan kebiasaan dalam menggunakan perangkat lunak yang sah (software security) memengaruhi tingkat kesadaran mereka terhadap ancaman digital. Faktor-faktor tersebut memainkan peran penting dalam menentukan tingkat kesadaran keamanan siber masyarakat.

Dalam menghadapi tantangan keamanan siber, pengguna yang lebih tua menunjukkan kecenderungan untuk fokus pada keamanan digital dengan membuat

kata sandi yang kuat dan memperbarui perangkat secara rutin, namun sering kali mengabaikan aspek keamanan fisik, seperti mengunci layar perangkat mereka (Branley-Bell et al., 2022). Sebaliknya, generasi muda lebih akrab dengan teknologi digital tetapi terkadang mengabaikan langkah-langkah keamanan mendasar, seperti menggunakan kata sandi yang unik atau memverifikasi sumber informasi sebelum membukanya. Hal ini menunjukkan perlunya pendekatan yang disesuaikan untuk meningkatkan kesadaran keamanan digital di setiap generasi.

Dibandingkan dengan populasi muda, orang tua cenderung kurang waspada terhadap tanda-tanda kecurangan atau penipuan digital (Yu et al., 2022), Hal ini sebagian besar disebabkan oleh tingkat kepercayaan yang lebih tinggi pada orang lain dan kebiasaan mereka untuk melihat interaksi sosial dalam konteks yang lebih positif. Seringkali, orang tua lebih cenderung mempercayai informasi yang diterima melalui media atau dari sumber-sumber yang tampak meyakinkan, bahkan tanpa verifikasi lebih lanjut. . Oleh karena itu, diperlukan pendekatan yang disesuaikan untuk meningkatkan kesadaran keamanan siber di setiap generasi, dengan menekankan pentingnya edukasi tentang keamanan digital, pengelolaan kata sandi, dan penghindaran risiko dalam komunikasi online. Generasi Milenial, dengan paparan teknologi sejak usia dini, memiliki potensi lebih besar untuk meningkatkan kesadaran keamanan digital dibandingkan generasi sebelumnya.

Generasi milenial (18-25 tahun) tumbuh besar di era digital sehingga lebih terbiasa dan paham mengenai bahaya di internet. Mereka tumbuh sambil mengakses internet sejak usia dini untuk menunjang kebutuhan belajar maupun hiburan (Hong et al., 2023). Oleh karena itu, generasi milenial sangat familiar dengan teknologi digital dan media sosial. Hal tersebut yang membedakan generasi milenial dengan generasi dewasa dalam hal kesadaran akan ancaman keamanan internet modern. Pengalaman di era digital membuat milenial lebih tanggap terhadap perkembangan dunia maya. Kebiasaan generasi milenial yang tumbuh di era digital membuat mereka lebih terpapar pada teknologi dan media sosial, sebuah tren yang sejalan dengan pesatnya peningkatan jumlah pengguna smartphone di Indonesia, yang kini hampir mencakup tiga perempat dari populasi.



Gambar 1.3 Jumlah Pengguna Smartphone di Indonesia 2023

Sumber : GoodStats (2023)

Jumlah pengguna smartphone di Indonesia terus mengalami peningkatan yang sangat pesat. Pada tahun 2023, diperkirakan ada sekitar 209,3 juta pengguna smartphone aktif, sebuah lonjakan besar dibandingkan dengan 54 juta pada tahun 2015. Hal ini menunjukkan bahwa hampir tiga perempat dari populasi Indonesia kini mengandalkan smartphone untuk berbagai kegiatan, mulai dari berkomunikasi, berbelanja online, hingga mengakses media sosial. Seiring dengan pesatnya pertumbuhan jumlah pengguna smartphone di Indonesia, penting untuk memahami bagaimana hal ini berdampak pada kesadaran dan perilaku keamanan siber, mengingat semakin banyaknya aktivitas digital yang dilakukan melalui perangkat ini.

Di Indonesia, penelitian ini relevan karena memberikan wawasan mengenai faktor-faktor yang memengaruhi kesadaran keamanan siber *(cybersecurity awareness)*, seperti pengetahuan keamanan siber (*cybersecurity knowledge*), keamanan kata sandi (password security), keamanan email (email security), persepsi individu terhadap keterampilan mereka sendiri (self-perception of skills), dan keamanan perangkat lunak (software security). Kesadaran keamanan siber menjadi semakin penting dalam menghadapi ancaman digital yang terus berkembang, terutama dengan tingginya tingkat penetrasi internet di Indonesia. Dengan menganalisis hubungan variabel-variabel tersebut, penelitian ini bertujuan

memberikan solusi untuk menciptakan lingkungan digital yang lebih aman bagi semua generasi.

Penelitian ini berfokus pada analisis hubungan antara faktor-faktor di atas dengan kesadaran keamanan siber masyarakat Indonesia, serta bagaimana sikap keamanan siber (cybersecurity attitude) memediasi hubungan tersebut. Dengan mengkaji aspek sikap, pengetahuan, dan perilaku masyarakat terkait keamanan digital, penelitian ini bertujuan untuk mengidentifikasi pola-pola yang memengaruhi kesadaran keamanan siber. Hasil penelitian ini diharapkan dapat memberikan rekomendasi praktis untuk meningkatkan keamanan digital di masyarakat Indonesia, baik melalui edukasi, kampanye publik, maupun kebijakan yang lebih terarah. Selain itu, penelitian ini juga berkontribusi dalam mendukung upaya menciptakan lingkungan digital yang lebih aman dan terlindungi dari ancaman kejahatan siber.

1.2 Latar Belakang Penelitian

Perkembangan teknologi informasi dan kemudahan akses internet telah mengubah cara manusia berinteraksi, berbisnis, hingga belajar. Namun, di balik kemajuan ini, muncul tantangan besar berupa meningkatnya ancaman keamanan digital. Menurut (Cremer et al., 2022), digitalisasi telah memperluas ruang kejahatan siber, sehingga diperlukan sistem keamanan yang tangguh di semua level, baik individu, organisasi, maupun negara.

Gambar 1.4 Jumlah Serangan Siber di Indonesia

Sumber : Edavos (2023)

Di Indonesia, tren serangan siber menunjukkan lonjakan signifikan. (Edavos, 2023) melaporkan bahwa terdapat 361 juta serangan siber pada Januari–Oktober 2023. Kasus kebocoran data 1,3 miliar SIM card pada tahun 2022 semakin menegaskan lemahnya pengamanan data digital. Selain itu, BSSN mencatat lebih dari 200 juta serangan siber pada semester pertama 2022, dengan sektor pemerintahan dan pelayanan publik sebagai sasaran utama. Surfshark melalui Katadata (2024) juga menunjukkan bahwa 94,22 juta akun di Indonesia terdampak kebocoran data selama 2020–2024, menempatkan Indonesia pada peringkat kedelapan dunia.

Gambar 1.5 Negara dengan Kebocoran Data Terbesar

Sumber : katadata.com (2024)

Masalah ini diperburuk oleh rendahnya kesadaran keamanan siber *(cybersecurity awareness)*. Banyak individu dan organisasi belum memiliki pemahaman memadai untuk menghadapi ancaman digital. Hal ini berdampak serius, mulai dari kerugian finansial, hilangnya kepercayaan konsumen, hingga instabilitas sosial. Chidukwani et al. (2024) menegaskan bahwa pelaku UKM yang belum memiliki sistem keamanan yang baik sangat rentan terhadap kebocoran data.

Oleh karena itu, penting untuk memahami faktor-faktor yang memengaruhi kesadaran keamanan siber.

Salah satu faktor penting adalah *cybersecurity knowledge*, yaitu sejauh mana seseorang memahami konsep, risiko, dan cara melindungi diri dari ancaman digital. Penelitian oleh Rahman et al. (2020) menunjukkan bahwa kurangnya pengetahuan dasar membuat generasi muda sangat rentan terhadap penipuan daring dan eksploitasi data pribadi. Pengetahuan yang kuat diyakini dapat mendorong individu untuk lebih waspada dan aktif dalam menjaga keamanan digitalnya.

Faktor berikutnya adalah password security. Banyak masyarakat Indonesia masih menggunakan kata sandi yang lemah dan berulang. Rasidi (2023) menegaskan bahwa hal ini menjadi celah besar dalam sistem keamanan digital. Studi oleh Branley-Bell et al. (2022) juga menunjukkan bahwa generasi muda cenderung abai terhadap praktik keamanan sandi, meskipun aktif dalam dunia digital. Keamanan kata sandi menjadi elemen dasar namun krusial dalam menjaga data pribadi.

Selanjutnya, self-perception of skills turut memengaruhi kesadaran digital. Individu yang merasa mampu menggunakan teknologi belum tentu memiliki kesadaran terhadap risikonya. Patel & Saini (2021) dalam studi di India menunjukkan bahwa persepsi terhadap kemampuan digital tidak selalu sejalan dengan perilaku aman. Hal ini juga tercermin di Indonesia, di mana generasi Z yang paling aktif secara digital justru sering mengabaikan praktik keamanan dasar.

Faktor keempat, yaitu email security, menjadi perhatian utama karena serangan phishing masih menjadi penyebab kebocoran data terbanyak menurut BSSN (2023). Bordonaba-Juste et al. (2020) menyatakan bahwa pengguna yang pernah menjadi korban phishing sering kali tetap lengah, terutama jika tidak dibarengi dengan edukasi yang berkelanjutan. Penguatan sistem dan kesadaran terhadap keamanan email sangat krusial mengingat email adalah pintu masuk utama berbagai layanan digital.

Selain itu, software security juga memainkan peran penting. Perangkat lunak yang tidak diperbarui membuka celah bagi pelanggaran data. Penelitian oleh Candiwan et al. (2023) menunjukkan bahwa praktik keamanan perangkat lunak

yang buruk berdampak langsung pada tingginya jumlah insiden dan kerugian. Sayangnya, banyak pengguna masih mengabaikan pembaruan sistem yang seharusnya menjadi langkah preventif utama.

Di antara semua faktor tersebut, cybersecurity attitude dapat menjadi mediator yang penting dalam membentuk kesadaran keamanan digital. Sikap terhadap keamanan digital memengaruhi sejauh mana seseorang menerapkan pengetahuan yang dimiliki ke dalam tindakan nyata. Studi oleh Wibowo & Susanto (2023) menunjukkan bahwa meskipun mahasiswa memiliki pengetahuan teknis, mereka tetap melakukan kesalahan dasar akibat kurangnya sikap protektif. Penelitian oleh Ramadhan et al. (2022) di kalangan ASN juga menemukan bahwa tingginya insiden phishing berkaitan erat dengan lemahnya sikap dan kontrol internal terhadap keamanan digital.

Meskipun isu ini semakin penting, penelitian mengenai pengaruh faktor-faktor seperti pengetahuan, perilaku kata sandi, persepsi kemampuan, keamanan email, dan software terhadap kesadaran keamanan siber di Indonesia masih terbatas. Terutama, peran sikap sebagai mediator jarang dieksplorasi dalam konteks lokal yang mempertimbangkan generasi digital dan kebiasaan masyarakat Indonesia.

Di Malaysia, dalam penelitian yang dilakukan oleh (Zulkifli et al., 2024) didapatkan hasil bahwa kampanye kesadaran siber telah menunjukkan hasil yang sangat positif, dengan fokus utama pada peningkatan pemahaman terkait ancaman seperti phishing, malware, ransomware, dan cyberbullying. Keberhasilan kampanye ini tercermin dari peningkatan signifikan dalam kesadaran siswa, yang terlihat melalui hasil survei dan uji coba yang dilakukan setelah program dilaksanakan.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengisi kesenjangan yang ada dengan mengeksplorasi pengaruh *cybersecurity knowledge*, password security, self-perception of skills, email security, dan software security terhadap cybersecurity awareness, serta menganalisis peran mediasi dari cybersecurity attitude. Penelitian ini diharapkan memberikan kontribusi praktis dalam menyusun strategi edukasi yang efektif serta masukan bagi kebijakan

keamanan digital di Indonesia. Karya ilmiah ini akan dituangkan dalam penelitian berjudul "Pengaruh *Cybersecurity Knowledge* dan Faktor Lain terhadap *Cybersecurity Awareness* dengan Mediasi *Cybersecurity Attitude* pada Masyarakat Indonesia."

1.3 Perumusan Masalah

Penelitian ini berfokus pada pentingnya memberdayakan masyarakat Indonesia dalam meningkatkan kesadaran keamanan siber *(cybersecurity awareness)* di tengah pesatnya perkembangan era digital. Setiap generasi memiliki tingkat pemahaman, keterampilan, dan sikap yang berbeda terhadap ancaman siber, yang memengaruhi kemampuan mereka dalam menjaga privasi dan keamanan informasi pribadi secara online. Dengan mengidentifikasi pengaruh pengetahuan keamanan siber (*cybersecurity knowledge*), faktor lain seperti pengelolaan kata sandi dan persepsi keterampilan, serta peran sikap keamanan siber (cybersecurity attitude) sebagai mediator, penelitian ini bertujuan untuk memahami bagaimana membangun kesadaran keamanan siber yang efektif di berbagai lapisan masyarakat.

Selain itu, penelitian ini mengeksplorasi dampak dari rendahnya kesadaran keamanan siber, khususnya di kalangan masyarakat, yang menjadi salah satu kelompok rentan terhadap ancaman digital. Keterbatasan pengetahuan, kelemahan dalam pengelolaan kata sandi, persepsi keterampilan yang rendah, serta kurangnya perhatian terhadap keamanan email dan perangkat lunak menjadi faktor yang memengaruhi kesadaran keamanan mereka, . Maka, penelitian ini juga menekankan pentingnya sikap positif terhadap keamanan siber sebagai elemen kunci dalam menghubungkan pengetahuan dan keterampilan dengan praktik keamanan digital. Maka dari itu dirumuskan pertanyaan penelitian berdasarkan variable diatas :

1. Apakah Pengetahuan Keamanan Siber (*Cybersecurity Knowledge*) berpengaruh terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness*)?
2. Apakah Keamanan Kata Sandi (*Password Security*) berpengaruh terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness*)?

3. Apakah Persepsi Diri Terhadap Keterampilan (*Self-Perception Of Skills*) berpengaruh terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness*)?
4. Apakah Keamanan Perangkat Lunak (*Software Security*) berpengaruh terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness*)?
5. Apakah Keamanan Email (*Email Security*) berpengaruh terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness*)?
6. Apakah sikap terhadap keamanan siber (*Cybersecurity Attitude*) memediasi pengaruh Pengetahuan Keamanan Siber terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness*)?
7. Apakah Sikap terhadap Keamanan Siber (*Cybersecurity Attitude*) memediasi pengaruh Keamanan Kata Sandi terhadap Kesadaran Keamanan Siber?
8. Apakah Sikap terhadap Keamanan Siber (*Cybersecurity Attitude*) memediasi pengaruh Persepsi Diri terhadap Keterampilan terhadap Kesadaran Keamanan Siber?
9. Apakah Sikap terhadap Keamanan Siber (*Cybersecurity Attitude*) memediasi pengaruh Keamanan Email terhadap Kesadaran Keamanan Siber?
10. Apakah Sikap terhadap Keamanan Siber (*Cybersecurity Attitude*) memediasi pengaruh Keamanan Perangkat Lunak terhadap Kesadaran Keamanan Siber?

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah dan pertanyaan penelitian yang sudah dijelaskan, maka tujuan pada penelitian ini adalah :

1. Untuk Mengetahui pengaruh Pengetahuan Keamanan Siber (*Cybersecurity Knowledge)* terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness)*
2. Untuk mengetahui pengaruh Keamanan Kata Sandi (*Password Security)* terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness)*

3. Untuk mengetahui pengaruh Persepsi Diri Terhadap Keterampilan (*Self-Perception Of Skills*) terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness)*
4. Untuk mengetahui pengaruh Keamanan Perangkat Lunak (*Software Security)* terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness)*
5. Untuk mengetahui pengaruh Keamanan Email (*Email Security)* terhadap Kesadaran Keamanan Siber (*Cybersecurity Awareness)*
6. Untuk mengetahui peran mediasi *Cybersecurity Attitude* dalam pengaruh *Cybersecurity Knowledge* terhadap *Cybersecurity Awareness*.
7. Untuk mengetahui peran mediasi *Cybersecurity Attitude* dalam pengaruh *Password Security* terhadap *Cybersecurity Awareness*.
8. Untuk mengetahui peran mediasi *Cybersecurity Attitude* dalam pengaruh *Self-Perception of Skills* terhadap *Cybersecurity Awareness*.
9. Untuk mengetahui peran mediasi *Cybersecurity Attitude* dalam pengaruh *Software Security* terhadap *Cybersecurity Awareness*.
10. Untuk mengetahui peran mediasi *Cybersecurity Attitude* dalam pengaruh *Email Security* terhadap *Cybersecurity Awareness*.

1.5 Manfaat Penelitian

Penelitian ini bertujuan untuk menganalisis pengaruh *Cybersecurity Knowledge*, *Password Security*, *Self-Perception of Skills*, *Software Security*, dan *Email Security* terhadap *Cybersecurity Awareness*, dengan *Cybersecurity Attitude* sebagai variabel mediasi pada masyarakat Indonesia. Dengan memahami hubungan antara faktor-faktor tersebut, penelitian ini diharapkan dapat mendorong peningkatan kesadaran keamanan siber di berbagai kalangan masyarakat Indonesia, terutama dalam menghadapi ancaman yang semakin kompleks di era digital.

Penelitian ini memberikan manfaat teoritis dalam memperkaya literatur terkait kesadaran keamanan siber, khususnya dengan pendekatan yang mengintegrasikan aspek pengetahuan, perilaku, dan sikap. Temuan dari penelitian ini akan memberi gambaran tentang bagaimana faktor teknis dan psikologis dapat memengaruhi perilaku aman digital di Indonesia. Hal ini dapat menjadi landasan

untuk penelitian selanjutnya yang lebih mendalam, seperti pengembangan model intervensi pendidikan keamanan siber berbasis generasi atau tingkat risiko.

Secara praktis, hasil penelitian ini dapat diimplementasikan dalam beberapa cara:

1. Penyusunan Modul Edukasi Keamanan Siber

   Temuan penelitian dapat dijadikan dasar dalam menyusun materi pelatihan atau modul literasi digital yang lebih tepat sasaran, misalnya untuk pelajar, mahasiswa, ASN, hingga pelaku UMKM. Modul ini bisa menekankan pentingnya pengelolaan kata sandi, mengenali serangan phishing, dan kebiasaan update perangkat lunak.

2. Kampanye Digital dengan Segmentasi Generasi

   Pemerintah dan penyedia layanan digital dapat menggunakan hasil penelitian untuk mendesain kampanye peningkatan kesadaran keamanan siber yang disesuaikan dengan karakteristik generasi—misalnya kampanye visual di media sosial untuk generasi muda, dan pelatihan langsung untuk generasi yang lebih tua.

3. Pengembangan Dashboard Penilaian Kesadaran Siber

   Organisasi atau lembaga pendidikan dapat mengembangkan alat ukur sederhana untuk menilai tingkat cybersecurity awareness dan attitude pegawai atau siswa. Dashboard ini bisa digunakan untuk memetakan kebutuhan pelatihan keamanan digital.

4. Penguatan Kebijakan Keamanan Digital di Lembaga Publik dan Swasta

   Hasil penelitian ini dapat dijadikan referensi untuk merumuskan kebijakan internal terkait praktik keamanan siber, seperti aturan rotasi kata sandi, kewajiban pembaruan sistem, atau pelatihan berkala bagi staf.

5. Program Pelatihan Berbasis Perilaku dan Sikap

   Dengan temuan bahwa sikap (attitude) dapat menjadi mediator penting, maka program pelatihan tidak cukup hanya bersifat teknis, melainkan juga perlu menyasar pembentukan kesadaran dan sikap protektif. Pelatihan dapat dilengkapi dengan simulasi kasus phishing atau studi dampak nyata dari kelalaian keamanan digital.

Dengan implementasi yang tepat, penelitian ini dapat memberikan kontribusi nyata bagi masyarakat dan lembaga dalam membangun ekosistem digital yang lebih aman dan adaptif terhadap risiko siber yang terus berkembang di Indonesia.