BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Gambaran Umum Lokasi Penelitian

1. Sejarah Fakultas Ilmu Sosial UIN Sumatera Utara

Salah satu tujuan Fakultas Ilmu Sosial adalah menghasilkan sarjana yang menguasai teori-teori sosial, termasuk didalamnya metode penelitian sosial, serta mampu menerapkannya dalam kegiatan penelitian. Untuk mewujudkan tujuan tersebut dirancang kurikulum dalam empat Program Studi yakni Ilmu Perpustakaan, Ilmu Komunikasi, Sejarah Peradaban Islam dan Prodi Sosiologi Agama

2. Visi dan Misi

Visi

Menjadi Fakultas unggulan yang menghasilkan sarjana yang profesional dalam bidang ilmu-ilmu sosial, terintegritas dengan nilai-nilai Islam,berdaya saing dan Berkarakter Islam.

Misi

a. Melaksanakan proses pendidikan dan pembelajaran dalammenyiapkan tenaga profesional dalam bidang ilmu-ilmu sosial sesuai standar pendidikan Nasional.
b. Melaksanakan penelitian untuk pengembangan ilmu-ilmu sosial.
c. Menemukan solusi terhadap masalah-masalah sosial yang berkembang.
d. Menyelenggarakan pelayanan kepada masyarakat melalui penerapanilmu-ilmu sosial.
e. Menyelenggarakan kerja sama kelembangan dengan berbagai pihakbaik dalam maupun luar negeri.
f. Membina karakter mahasisiwa sehingga sesuai dengan nilai-nilaiIslam.

B. Deskripsi Responden

1. Deskripsi Karakteristik Responden Berdasarkan Jenis Kelamin

Tabel 4.2 Deskripsi Karakteristik Responden Berdasarkan Jenis Kelamin

NO	Jenis Kelamin	Jumlah Mahasiswa	Persentase Responden
1	Laki-laki	15	23,4%
2	Perempuan	49	76,6%
Total		**64**	**100%**

Berdasar jenis kelamin terdapat 15 responden yang berjenis kelamin laki- laki dengan persentase 23.4% dan juga perempuan dengan total 49 responden dengan persentase 76.6% total keseluruhan adalah 64 responden dengan presentase 100%.

2. Deskripsi Karakteristik Responden Berdasarkan Usia

Tabel 4.3 Deskripsi Karakteristik RespondenBerdasarkan Usia

NO	Usia	Jumlah Mahasiswa	Persentase Responden
2	21	33	51,6 %
3	22	31	48,4 %
Total		**64**	**100%**

Pada tabel ini diketahui responden yang berusia 21 tahun berjumlah 33 responden dengan persentase 51,6 %, berusia 22 tahun berjumlah 31 responden dengan persentase 48,4%. maka total keseluruhan responden adalah 64 responden dengan persentase 100%.

C. Hasil Penelitian

1. Tingkat Kesadaran Informasi Mahasiswa Prodi Ilmu Perpustakaan Stambuk 2020-2021 Universitas Islam Negeri Sumatera Utara Dalam Bersosial Media

Berdasarkan kuesioner yang telah disebar terhadap 64 responden, data pengolahan statistik yang diperoleh dengan bantuan *SPSS* maka tabel pengkategorian kecenderungan variabel kesadaran adalah sebagai berikut:

Tabel 4.4 Pengkategorian Indikator Attitude

Item Pernyataan	N	Skor	Tingkat Capaian Responden (TCR) %	Kategori
X1.1	64	274	85,62	Baik
X1.2	64	275	85,93	Baik
X1.3	64	289	90,31	Baik
X1.4	64	278	86,87	Baik
X1.5	64	288	90	Baik
Rata-rata			87,75	Baik

Pada indikator attitude terdapat 5 butir item pernyataan yang digunakan sebagai data penelitian, yang mana keamanan data yang diinput dari orang yang tidak berhak mengakses (X1.1) memiliki nilai persentase sebesar 85.62% dan berada dalam kategori baik. Selanjutnya mengenai sistem back-up yang bagus (X1.2) memiliki nilai persentase sebesar 85.93% dan berada dalam kategori baik. Kemudian data tidak hilang meskipun listrik mati mendadak (X1.3) berada dalam kategori baik dengan persentase sebesar 90.31%. Lalu data tidak akan hilang meskipun smartphone rusak (X1.4) berada dalam kategori baik dengan persentase sebesar 86.87%. Kemudian yang terakhir yaitu sistem informasi jarang crash (X1.5) berada dalam kategori baik dengan persentase sebesar 90%. Selanjutnya dari kelima butir pernyataan tersebut didapat rata-rata sebesar 87.75% maka dalam indikator attitude diketahui berada dalam kategori baik.

Tabel 4.4 Pengkategorian Indikator Knowladge

Item Pernyataan	N	Skor	Tingkat Capaian Responden (TCR) %	Kategori
X2.1	64	276	86,25	Baik
X2.2	64	276	86,25	Baik
X2.3	64	294	91,87	Baik
X2.4	64	279	87,18	Baik
X2.5	64	285	89,06	Baik
Rata-rata			88,12	Baik

Pada indikator knowledge terdapat 5 butir item pernyataan yang digunakan sebagai data penelitian, yang mana serangan akses mencuri data pribadi (X2.1) memiliki nilai persentase sebesar 86.25% dan berada dalam kategori baik. Selanjutnya mengenai smartphone yang tertanam backdoor (X2.2) memiliki nilai persentase sebesar 86.25% dan berada dalam kategori baik. Kemudian pengunduhan aplikasi pada situs resmi (X2.3) berada dalam kategori baik dengan persentase sebesar 91.87%. selanjutnya mengenai hak akses (X2.4) berada dalam kategori baik dengan persentase sebesar 87.18%. Kemudian yang terakhir yaitu mengenai sertifikasi OEM dan lulus Build Test Suite (X2.5) berada dalam kategori baik dengan persentase sebesar 89.06%. Selanjutnya dari kelima butir pernyataan tersebut didapat rata-rata sebesar 88.12% maka dalam indikator knowledge diketahui berada dalam kategori baik.

Tabel 4.5 Pengkategorian Indikator Behaviour

Item Pernyataan	N	Skor	Tingkat Capaian Responden (TCR) %	Kategori
X3.1	64	280	87,5	Baik
X3.2	64	272	85	Baik
X3.3	64	296	92,5	Baik
X3.4	64	287	89,68	Baik
X3.5	64	286	89,37	Baik
Rata-rata			88,81	Baik

Pada indikator attitude terdapat 5 butir item pernyataan yang digunakan sebagai data penelitian, yang mana yaitu serangan berbasis backdoor (X3.1) memiliki nilai persentase sebesar 87,50% dan berada dalam kategori baik. Selanjutnya mengenai smartphone yang tertanam backdoor (X3.2) memiliki nilai persentase sebesar 85% dan berada dalam kategori baik. Kemudian pengunduhan aplikasi pada situs resmi (X3.3) berada dalam kategori baik dengan persentase sebesar 92.50%. selanjutnya mengenai hak akses (X3.4) berada dalam kategori baik dengan persentase sebesar 89.68%. Kemudian yang terakhir yaitu mengenai sertifikasi OEM dan lulus Build Test Suite (X3.5) berada dalam kategori baik dengan persentase sebesar 89.37%. Selanjutnya dari kelima butir pernyataan tersebut didapat rata-rata sebesar 88.82% maka dalam indikator behavior diketahui berada dalam kategori baik.

Tabel 4.5 Pengkategorian Variabel Keamanan

Item Pernyataan	N	Skor	Tingkat Capaian Responden (TCR) %	Kategori
Y1.1	64	272	85	Baik
Y1.2	64	268	83,75	Baik
Y1.3	64	295	92,18	Baik
Y1.4	64	276	86,25	Baik
Y1.5	64	280	87,5	Baik
Rata-rata			86, 93	Baik

Pada indikator keamanan terdapat 5 butir item pernyataan yang digunakan sebagai data penelitian, yang mana yaitu Langkah pencegahan terhadap serangan *backdoor* di smartphone android (Y1.1) memiliki nilai persentase sebesar 85% dan berada dalam kategori baik. Selanjutnya mengenai penghindaran smartphone dengan *backdoor* dari pabrik (Y1.2) memiliki nilai persentase sebesar 3.75% dan berada dalam kategori baik. Kemudian pengunduhan aplikasi pada situs resmi (Y1.3) berada dalam kategori baik dengan persentase sebesar 92.18%. Selanjutnya mengenai Pertimbangan hak akses aplikasi (Y1.4) berada dalam kategori baik dengan persentase sebesar 86.25%. Kemudian yang terakhir yaitu mengenai sertifikasi OEM dan lulus Build Test Suite (Y1.5) berada dalam kategori baik dengan persentase sebesar 87.50%. Selanjutnya dari kelima butir pernyataan tersebut didapat rata-rata sebesar 86.93% maka dalam indikator keamanan diketahui berada dalam kategori baik.

Dengan demikian berdasarkan ketiga indikator tersebut yaitu attitude, knowledge dan behaviour diperoleh rekapitulasi yang akan disajikan dalam tabel berikut:

Tabel 4.6 Rekapitulasi Pengukuran Tingkat Kesadaran akan Keamanan Informasi

Indikator	**N**	**Rata-rata masing-masing indikator**	**Kategori**
Attitude	64	87,75	Baik
Knowledge	64	88,12	Baik
Behaviour	64	88,81	Baik
Rata-rata		**88.82**	**Baik**

Berdasarkan tabel tersebut diperoleh rata-rata persentase sebesar 88.82% dan berada dalam kategori baik. Yang mana dilihat berdasarkan indikator Attitude dengan presentase 87.75% (kategori baik), Knowledge dengan presentase 88.12% (kategori baik), dan Behaviour 88.81% (kategori baik).

D. Analisis Data

1. Uji Asumsi Klasik

a. Uji Normalitas

Uji normalitas *kolmogorov-smirnov* merupakan bagian dari uji asumsi klasik yang bertujuan untuk mengetahui apakah nilai residual berdistribusi normal atau tidak. Adapun hasil pengujian uji normalitas yang didapat adalah sebagai berikut:

Tabel 4.27 Hasil Uji Normalitas *(Kolmogorov-Smirnov)*

One-Sample Kolmogorov-Smirnov Test

		Unstandardized Residual
N		64
Normal Parameters[a,b]	Mean	.0000000
	Std. Deviation	1.83299127
Most Extreme Differences	Absolute	.099
	Positive	.083
	Negative	-.099
Test Statistic		.099
Asymp. Sig. (2-tailed)		.198[c]

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

Uji normalitas diperlukan sebagai syarat uji untuk analisis regresi. Pada uji ini dasar pengambilan keputusan dilihat dari nilai signifikansi yang dapat diperoleh dari uji SPSS.

- Jika nilai signifikansi > 0.05 maka nilai residual berdistribusi morma
- Jika nilai signifikansi < 0.05 maka nilai residual tidak berdistribusi normal

Berdasarkan hasil uji normalitas diketahui nilai signifikansi 0.198 > 0.05 maka dapat disimpulkan bahwa nilai residual berdistribusi morma. Maka dari itu, pengujian asumsi klasik dapat dilanjutkan dengan tahap uji liniearitas.

b. Uji Liniearitas

Uji liniearitas bertujuan untuk mengetahui hubungan antara variabel bebas dengan variabel terikat. Pada uji ini akan terlihat hubungan yang linier

(garis lurus). Adapun hasil pengujian liniearitas pada data penelitian ini adalah sebagai berikut:

Tabel 4.28 Hasil Uji Liniearitas

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	120.813	1	120.813	35.387	.000[b]
	Residual	211.671	62	3.414		
	Total	332.484	63			.443

Adapun dasar pengambilan keputusannya adalah sebagai berikut:

- Jika nilai Sig. deviation from liniearity > 0.05, maka terdapat hubungan yang linier antara variabel bebas dengan variabel terikat
- Jika nilai Sig. deviation from liniearity < 0.05, maka tidak terdapat hubungan yang linier antara variabel bebas dengan variabel terikat.

Berdasarkan hasil uji liniearitas diketahui nilai *Sig. deviation from liniearity* sebesar 0.443 > 0.05, maka dapat disimpulkan bahwa terdapat hubungan yang linier antara kesadaran dengan tingkat keamanan informasi. Diketahui bahwasanya kedua syarat untuk analisis regresi linier sudah terpenuhi, maka dilanjutkan dengan uji analisis regresi sederhana.

2. Analisis Regresi Linier Sederhana

Analisis regresi linier sederhana digunakan sebagai cara untuk menguji ada tidaknya pengaruh antara variabel bebas dengan variabel terikat. Adapun syarat untuk melakukan uji ini adalah jenis data yang digunakan harus valid dan reliabel, berdistribusi normal dan memiliki hubungan yang linier (garis lurus).

Dasar pengambilan keputusan dalam uji ini mengacu pada dua hal yaitu:

Dengan membandingkan nilai signifikansi dengan probabilitas 0.05

- Jika nilai signifikansi < 0.05, maka dapat diartikan variabel X berpengaruh terhadap variabel Y

  Membandingkan nilai t_{hitung} dengan t_{tabel}
- Jika nilai $t_{hitung} > t_{tabel}$ maka variabel X berpengaruh terhadap variabel Y

- Jika nilai $t_{hitung} < t_{tabel}$ maka variabel X tidak berpengaruh terhadap variabel Y

Adapun hasil uji analisis regresi linier sederhana dalam pengujian menggunakanSPSS adalah sebagai berikut :

Tabel 4.29 Hasil Uji Analisis Linier Sederhana

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	-3.250	4.206		-.773	.443
	Kesadaran	1.134	.191	.603	5.949	.000

a. Dependent Variable: Tingkat Kesadaran

Diketahui nilai constant (a) sebesar -3.250 sedangkan nilai Kesadaran (b/ koefisien regresii) sebesar 1.134 sehingga persamaan regresi nya dapat ditulis:

Y = a + bX

Y = -3.250+ 1.134X

Persamaan tersebut dapat diterjemahkan sebagai berikut:

- Konstanta sebesar -3.250 mengandung arti bahwa nilai konsisten variabeltingkat kesadaran sebesar -3.250
- Koefisien regresi X sebesar 1.134 menyatakan bahwa setiap penambahan 1% nilai keamanan informasi, maka nilai tingkat kesadaran bertambah sebesar 1.134. koefisien regresi terebut bernilai positif sehingga dapat dikatakan bahwaarah pengaruh variabel X dan Y adalah positif

Berdasarkan nilai sig dari tabel coefficients diperoleh nilai signifikansinya sebesar 0.000 < 0.05, sehingga dapat disimpulkan bahwa variabel Tingkat Kesadaran (X) berpengaruh terhadap Keamanan informasi (Y).

Berdasarkan nilai t diketahui nilai t_{hitung} sebesar 5.949 > t_{tabel} -0.773 sehingga dapat disimpulkan bahwa variabel kesadaran (X) berpengaruh terhadap variabel tingkat keamanan informasi (Y)

E. Pembahasan

Dalam penelitian ini, salah satu fokus utama adalah mengevaluasi sikap atau *attitude, knowledge* dan *behaviour* mahasiswa Prodi Ilmu Perpustakaan Stambuk 2020-2021 Universitas Islam Negeri Sumatera Utara terhadap keamanan informasi, khususnya dalam konteks penggunaan media sosial. Sikap ini mencerminkan bagaimana mahasiswa merespons dan memperlakukan data pribadi mereka serta bagaimana mereka memandang berbagai aspek terkait perlindungan informasi

1. Tingkat Kesadaran Pengguna Akan Keamanan Informasi Dari Dimensi (*Attitude*) Mahasiswa Prodi Ilmu Perpustakaan UIN Sumatera Utara Dalam Bersosial Media

Dalam indikator *attitude*, berdasarkan hasil penelitian, sebesar 85,62% responden menyatakan bahwa data yang mereka input aman dari akses pihak yang tidak berhak. Ini menunjukkan bahwa mayoritas mahasiswa memiliki pemahaman yang baik mengenai pentingnya langkah-langkah keamanan, seperti enkripsi dan pembatasan akses. Tingkat kesadaran ini tergolong baik, mengindikasikan bahwa mahasiswa telah mempraktikkan protokol keamanan yang memadai.

Selanjutnya mengenai sikap ketika kehilangan data ketika pemadaman listrik, diketahui sebesar 90,31% responden yakin bahwa data mereka tidak akan hilang meskipun terjadi pemadaman listrik mendadak. Hal ini menandakan bahwa mahasiswa cenderung memilih perangkat atau sistem dengan fitur perlindungan data yang baik, atau mereka memahami pentingnya melakukan backup secara rutin. Kesadaran ini menunjukkan bahwa mereka memiliki pemahaman yang matang terkait risiko kehilangan data dan cara pencegahannya

Lalu dalam menilai sikap responden mengenai sistem informasi yang dipakai responden, sebanyak 90% responden mengakui bahwa sistem informasi yang mereka gunakan jarang mengalami crash. Hasil ini menunjukkan bahwa mahasiswa memahami pentingnya penggunaan sistem dengan arsitektur yang kuat dan pemeliharaan yang baik. Stabilitas sistem yang diandalkan ini berkontribusi pada rasa aman mahasiswa dalam mengakses informasi tanpa khawatir akan gangguan teknis yang berlebihan. Sejalan dengan penelitian yang dilakukan Mukhlis Amin (Amin, 2014), Kesadaran keaman informasi perlu terus ditingkatkan karena keamanan informasi bukan hanya persoalan teknikal saja,

namun konstribusi kelalaian manusia juga berpengaruh dalam kerentanan keamanan informasi.

Dapat disimpulkan bahwa, indikator *attitude* menunjukkan tingkat kesadaran yang baik terhadap keamanan informasi, dengan persentase sebesar 87,75%. Hal ini mencerminkan bahwa sebagian besar mahasiswa Prodi Ilmu Perpustakaan Stambuk 2020-2021 di Universitas Islam Negeri Sumatera Utara memiliki sikap yang positif dalam melindungi data pribadi mereka saat bersosial media. Keberhasilan dalam sub indikator seperti keamanan data dari akses yang tidak sah, keandalan backup data, ketahanan data terhadap gangguan listrik dan kerusakan perangkat, serta kestabilan sistem informasi, mengindikasikan bahwa mahasiswa memahami pentingnya menjaga integritas dan ketersediaan informasi. Kesimpulannya, kesadaran yang tinggi ini sangat mendukung upaya perlindungan data dan keamanan informasi mereka dalam bersosial media.

Selanjutnya akan dipaparkan lima sub indikator utama yang menggambarkan sikap mahasiswa terhadap keamanan informasi:

1. Hak Akses

   Pada sub indikator pertama, terdapat beberapa faktor penting yang mempengaruhi tingkat keamanan data. Salah satu faktor utama adalah penggunaan teknologi enkripsi yang kuat. Enkripsi berfungsi sebagai pelindung utama data dengan mengubah informasi menjadi kode rahasia yang hanya bisa dibaca oleh pihak yang memiliki kunci dekripsi. Dengan demikian, meskipun data tersebut jatuh ke tangan yang salah, isinya tetap tidak dapat diakses tanpa kunci yang tepat.

   Selain itu, autentikasi pengguna juga memainkan peran krusial. Sistem yang dilengkapi dengan metode autentikasi berlapis, seperti kata sandi yang kuat, autentikasi dua faktor (2FA), atau penggunaan biometrik, mampu memberikan perlindungan ekstra terhadap data. Hanya pengguna yang telah terverifikasi yang diizinkan mengakses data, sehingga kemungkinan akses oleh pihak yang tidak berwenang dapat diminimalkan.

   Faktor lain yang tidak kalah penting adalah penerapan kebijakan akses dan izin. Prinsip “least privilege” memastikan bahwa akses ke data hanya diberikan kepada pihak yang benar-benar memerlukannya, sehingga mengurangi risiko

data jatuh ke tangan yang salah. Di samping itu, keamanan jaringan juga berperan signifikan. Dengan adanya firewall dan sistem deteksi intrusi, sistem dapat menahan upaya akses dari pihak luar yang berpotensi membahayakan.

Kesadaran pengguna mengenai pentingnya menjaga kerahasiaan data juga menjadi kunci dalam melindungi informasi. Pengguna yang memiliki pengetahuan dan kesadaran tinggi tentang risiko keamanan informasi akan lebih berhati-hati dalam menginput dan menyimpan data mereka. Namun, jika data yang diinput tidak aman, ada beberapa akibat serius yang bisa terjadi. Salah satunya adalah kebocoran data pribadi. Informasi sensitif seperti alamat, nomor telepon, atau detail keuangan dapat bocor dan dimanfaatkan oleh pihak tidak bertanggung jawab untuk melakukan penipuan atau pencurian identitas. Selain itu, akses tidak sah ke data juga membuka peluang bagi penjahat siber untuk melancarkan serangan, seperti phishing atau ransomware.

Secara keseluruhan, menjaga keamanan data yang diinput dari akses pihak yang tidak berhak merupakan hal yang sangat penting. Dengan meminimalkan risiko kebocoran dan akses tidak sah, pengguna akan merasa lebih aman dan terlindungi, serta kepercayaan terhadap sistem yang digunakan dapat tetap terjaga. Berdasarkan hasil penelitian, sebesar 85,62% responden menyatakan bahwa data yang mereka input aman dari akses pihak yang tidak berhak. Ini menunjukkan bahwa mayoritas mahasiswa memiliki pemahaman yang baik mengenai pentingnya langkah-langkah keamanan, seperti enkripsi dan pembatasan akses. Tingkat kesadaran ini tergolong baik, mengindikasikan bahwa mahasiswa telah mempraktikkan protokol keamanan yang memadai.

2. Backup Data

Backup data yang baik merupakan salah satu aspek penting dalam menjaga keamanan informasi. Ada beberapa faktor yang mendukung keberhasilan sistem backup ini. Pertama, kesadaran pengguna menjadi faktor utama. Mahasiswa yang paham pentingnya menjaga data akan secara rutin melakukan backup, memastikan informasi penting mereka selalu aman. Kedua, perkembangan teknologi penyimpanan seperti cloud storage dan hard drive eksternal memudahkan proses backup. Dengan teknologi ini, data dapat disimpan secara otomatis dan aman. Kebijakan institusi yang mendukung

praktik backup juga berperan besar. Jika kampus atau program studi memberikan panduan serta alat untuk backup, maka kualitas backup yang dilakukan akan lebih baik. Selain itu, infrastruktur yang memadai, seperti koneksi internet yang stabil, memastikan proses sinkronisasi data ke cloud berjalan tanpa hambatan. Terakhir, kesesuaian sistem juga penting. Sistem yang dilengkapi fitur backup otomatis dan penyimpanan terdistribusi menjamin data tetap aman meskipun terjadi masalah pada satu lokasi penyimpanan.

Dampak dari backup data yang baik sangat signifikan. Pertama, ini meningkatkan keamanan data secara keseluruhan. Data yang dicadangkan secara rutin akan mengurangi risiko kehilangan informasi penting akibat kerusakan perangkat atau serangan siber. Ketika bencana terjadi, mahasiswa dapat dengan cepat memulihkan data yang hilang, sehingga aktivitas akademik mereka tidak terganggu. Hal ini juga mengurangi tingkat stres, karena mahasiswa merasa lebih tenang dengan jaminan bahwa data mereka aman. Selain itu, backup yang baik membantu memenuhi regulasi atau kebijakan terkait keamanan informasi, yang sering kali diwajibkan dalam lingkungan akademik. Keberlanjutan penggunaan sistem juga terjamin, karena sistem yang memiliki backup yang andal cenderung lebih tahan terhadap gangguan, memperpanjang umur pakainya dan meningkatkan kepercayaan pengguna.

Secara keseluruhan, backup data yang baik tidak hanya melindungi informasi, tetapi juga memastikan kelancaran aktivitas akademik dan keberlanjutan penggunaan sistem. Ini memberikan rasa aman bagi mahasiswa dan menjamin bahwa data mereka tetap terlindungi dari berbagai ancaman. Berdasarkan hasil penelitian, Sebanyak 85,93% responden menilai sistem yang mereka gunakan memiliki mekanisme backup data yang baik. Ini berarti mahasiswa memiliki pemahaman yang cukup tentang pentingnya menyimpan salinan data di lokasi berbeda untuk mencegah kehilangan data akibat kejadian tak terduga. Kesadaran ini penting untuk memastikan keberlanjutan akses informasi, bahkan dalam situasi darurat.

3. Pencegahan kehilangan data ketika smartphone rusak

Mahasiswa yang telah terbiasa menyinkronkan data mereka dengan layanan cloud seperti Google Drive, iCloud, atau Dropbox memiliki

keuntungan besar. Melalui sinkronisasi otomatis ini, data mereka tersimpan dengan aman di server cloud, sehingga jika perangkat fisik mengalami kerusakan, data tetap dapat diakses kapan saja dari perangkat lain.

Selain itu, backup data ke komputer atau perangkat penyimpanan eksternal juga menjadi salah satu langkah bijak yang dilakukan oleh sebagian besar mahasiswa. Dengan melakukan backup secara berkala, mereka memiliki cadangan fisik yang dapat diandalkan ketika smartphone mengalami masalah. Proses ini memastikan bahwa data penting tetap aman dan siap digunakan meskipun perangkat utama rusak.

Penggunaan kartu SD sebagai media penyimpanan tambahan juga tidak kalah penting. Dengan menyimpan data di kartu SD yang dapat dilepas, mahasiswa dapat dengan mudah memindahkan data tersebut ke perangkat lain jika smartphone mengalami kerusakan. Langkah ini memberikan lapisan perlindungan ekstra terhadap data mereka.

Dampak dari penerapan langkah-langkah ini sangat signifikan. Mahasiswa yang rutin menyinkronkan dan membackup data mereka tidak perlu khawatir kehilangan informasi penting saat smartphone rusak. Mereka dapat dengan mudah memulihkan data dari cloud atau perangkat cadangan lainnya, sehingga aktivitas sehari-hari tidak terganggu. Risiko kehilangan data secara permanen juga menjadi sangat kecil karena data tersebar di beberapa lokasi penyimpanan. Lebih dari itu, kesiapan mahasiswa dalam menghadapi insiden tak terduga, seperti kerusakan perangkat, mencerminkan kesadaran dan tanggung jawab yang tinggi terhadap manajemen data pribadi.

Dengan demikian, sub-indikator ini menunjukkan bahwa mahasiswa memiliki pemahaman yang kuat tentang pentingnya menjaga data mereka, dan langkah-langkah yang mereka ambil memberikan perlindungan yang memadai terhadap risiko kerusakan perangkat. Hal ini menandakan tingkat kesadaran yang baik dan kesiapan mereka dalam menjaga keamanan informasi di era digital. Berdasarkan hasil penelitian, 90,31% responden percaya bahwa data mereka tetap aman meskipun smartphone rusak. Hal ini menegaskan bahwa mahasiswa telah memanfaatkan teknologi seperti sinkronisasi dengan cloud, backup ke komputer, atau penggunaan kartu SD sebagai upaya mitigasi risiko

kehilangan data. Kesadaran ini mencerminkan pemahaman yang tinggi terhadap manajemen data pribadi.

4. Sistem informasi jarang crash

Sistem informasi yang jarang mengalami crash menunjukkan kualitas dan keandalan yang sangat penting dalam dunia digital saat ini. Untuk mencapai stabilitas ini, beberapa faktor kunci memainkan peran penting. Pertama, arsitektur sistem yang solid menjadi fondasi utama. Sistem yang dirancang dengan struktur yang kokoh antara perangkat keras dan perangkat lunak memastikan bahwa semua komponen bekerja secara harmonis. Ini berarti sistem dapat menangani berbagai beban kerja tanpa menghadapi gangguan yang signifikan. Ketika arsitektur sistem dirancang dengan baik, risiko terjadinya crash atau kerusakan teknis dapat diminimalkan, dan operasi sistem tetap konsisten.

Kedua, penggunaan perangkat keras dan perangkat lunak yang berkualitas tinggi juga sangat berpengaruh. Komponen yang terpilih dengan cermat dan terbaru memastikan performa sistem yang optimal. Ketika perangkat keras dan perangkat lunak saling mendukung dan kompatibel, kemungkinan terjadinya kegagalan teknis menjadi jauh lebih kecil. Hal ini berkontribusi pada stabilitas sistem secara keseluruhan, mengurangi kemungkinan gangguan atau crash yang tidak diinginkan.

Ketiga, pemeliharaan dan pembaruan sistem yang rutin tidak kalah penting. Dengan melakukan pembaruan perangkat lunak secara teratur, memperbaiki bug, dan mengoptimalkan kinerja, sistem tetap berada dalam kondisi terbaiknya. Pemeliharaan ini memastikan bahwa sistem terlindungi dari kerentanannya dan dapat mengatasi potensi masalah sebelum menjadi lebih serius. Dengan cara ini, risiko crash dapat dikurangi, dan sistem tetap berfungsi dengan baik.

Keempat, stabilitas jaringan juga berperan penting. Jaringan komputer yang cepat dan stabil mendukung kinerja sistem informasi, memungkinkan akses data dan komunikasi antar komponen berjalan lancar. Jaringan yang baik mengurangi keterlambatan dan gangguan dalam komunikasi data, membantu menjaga sistem tetap operasional dan mengurangi kemungkinan crash yang

disebabkan oleh masalah jaringan.

Kelima, adanya sistem backup yang efektif menjadi jaring pengaman yang tak kalah penting. Backup yang dilakukan secara teratur dan disimpan di lokasi aman memungkinkan pemulihan data yang cepat jika terjadi crash. Dengan sistem backup yang baik, dampak dari kegagalan sistem dapat diminimalisir, dan data tetap terlindungi.

Secara keseluruhan, stabilitas sistem informasi berkontribusi pada operasi yang efisien, pengalaman pengguna yang baik, dan perlindungan data yang solid. Menjaga sistem tetap stabil adalah kunci untuk sukses dalam dunia digital yang semakin bergantung pada teknologi. Sebanyak 90% responden mengakui bahwa sistem informasi yang mereka gunakan jarang mengalami crash. Hasil ini menunjukkan bahwa mahasiswa memahami pentingnya penggunaan sistem dengan arsitektur yang kuat dan pemeliharaan yang baik. Stabilitas sistem yang diandalkan ini berkontribusi pada rasa aman mahasiswa dalam mengakses informasi tanpa khawatir akan gangguan teknis yang berlebihan. Sejalan dengan penelitian yang dilakukan Mukhlis Amin (Amin, 2014), Kesadaran keaman informasi perlu terus ditingkatkan karena keamanan informasi bukan hanya persoalan teknikal saja, namun konstribusi kelalaian manusia juga berpengaruh dalam kerentanan keamanan informasi

2. Tingkat Kesadaran Pengguna Akan Keamanan Informasi Dari Dimensi Pengetahuan (K*nowledge*) Mahasiswa Prodi Ilmu Perpustakaan UIN Sumatera Utara Dalam Bersosial Media

Selanjutnya, pada indikator dalam kategori *knowledge* (pengetahuan) yang masing-masing menggambarkan pemahaman mahasiswa tentang berbagai risiko dan langkah-langkah pencegahan yang dapat diambil untuk melindungi data pribadi mereka, diketahui bahwa dalam pengetahuan responden mengenai potensi serangan pada smartphone yang dapat mencuri data pribadi. Hasil menunjukkan bahwa 86,25% dari responden memahami risiko ini dengan baik. Persentase ini menandakan bahwa mayoritas responden menyadari bahaya serangan seperti malware dan phishing yang dapat mempengaruhi smartphone mereka. Hal ini menunjukkan tingkat pemahaman yang baik tentang bagaimana smartphone dapat menjadi target serangan dan pentingnya menjaga keamanan data pribadi.

Selanjutnya, dalam menilai pengetahuan responden mengenai kemungkinan adanya *backdoor* pada smartphone yang sudah tertanam sejak pabrik. Sebanyak 86,25% responden menunjukkan kesadaran yang baik tentang keberadaan *backdoor* perangkat keras. Angka ini mencerminkan bahwa mereka memahami adanya risiko tambahan dari *backdoor* yang dapat digunakan untuk akses tidak sah dan pengumpulan data tanpa sepengetahuan pengguna.

Kemudian, dalam menilai pengetahuan responden tentang risiko aplikasi yang tidak diunduh dari Google Play Store atau repositori resmi. Dengan persentase 91,87%, responden menunjukkan pemahaman yang sangat baik tentang bahaya aplikasi dari sumber tidak resmi, termasuk potensi adanya malware atau *backdoor*. Persentase tinggi ini menunjukkan bahwa responden cenderung berhati-hati dalam memilih aplikasi dan memahami pentingnya mendownload aplikasi hanya dari sumber terpercaya.

Dalam mengevaluasi pengetahuan responden mengenai pentingnya memeriksa hak akses aplikasi sebelum menginstalnya. Dengan persentase 87,18%, sebagian besar responden menunjukkan pemahaman yang baik tentang perlunya mengevaluasi hak akses aplikasi. Ini menunjukkan bahwa mereka cenderung memperhatikan izin yang diminta aplikasi dan menyadari potensi risiko yang terkait dengan izin berlebihan.

Selanjutnya, 89,06% responden mengetahui bahwa smartphone dengan sertifikasi OEM umumnya lebih aman. Persentase ini mencerminkan bahwa responden memahami pentingnya memilih perangkat yang telah melalui pengujian keamanan yang ketat dan memiliki jaminan dari produsen.

Sehingga dapat disimpulkan, pada indikator *knowledge* memperoleh persentase sebesar 88.12% yang berada dalam kategori baik. Capaian ini dipengaruhi oleh kesadaran mahasiswa terhadap beberapa sub indikator penting, seperti potensi serangan backdoor pada smartphone, kemungkinan adanya backdoor perangkat keras yang tertanam pada firmware dari pabrik, risiko penggunaan aplikasi yang tidak diunduh dari sumber resmi, pertimbangan hak akses aplikasi sebelum instalasi, serta keamanan perangkat berdasarkan sertifikasi OEM dan pengujian Build Test Suite

Selanjutnya, lima sub indikator dalam kategori *knowledge* (pengetahuan)

yang masing-masing menggambarkan pemahaman mahasiswa tentang berbagai risiko dan langkah-langkah pencegahan yang dapat diambil untuk melindungi data pribadi mereka, akan dijabarkan sebagai berikut:

1. Pengetahuan terhadap serangan pada smartphone

   Penting untuk memahami bahwa smartphone, seperti perangkat digital lainnya, tidak kebal terhadap serangan siber. Mahasiswa perlu menyadari bahwa smartphone dapat menjadi target serangan yang dirancang untuk memberikan akses kepada penyerang dalam mencuri data pribadi. Kesadaran ini mencakup pemahaman tentang berbagai metode serangan yang mungkin dihadapi dan langkah-langkah yang dapat diambil untuk memitigasi risiko tersebut. Adapun faktor-faktor yang mempengaruhi kesadaran terhadap serangan pada smartphone diantaranya adalah:

   a. Pengetahuan Teknologi

      Pengetahuan dasar tentang bagaimana smartphone bekerja dan jenis-jenis serangan yang bisa terjadi sangat penting. Ketika seseorang memahami konsep dasar seperti malware, phishing, dan kerentanan sistem, mereka lebih cenderung untuk mengambil langkah-langkah pencegahan yang diperlukan. Misalnya, mereka akan lebih waspada terhadap aplikasi yang meminta izin yang tidak perlu atau link yang mencurigakan.

   b. Pengalaman Pribadi

      Pengalaman langsung dengan serangan atau ancaman dapat memperkuat kesadaran seseorang. Jika seseorang pernah mengalami serangan phishing atau malware yang merusak perangkat mereka, pengalaman tersebut akan menjadi pengingat kuat untuk lebih berhati-hati di masa depan. Pengalaman ini sering kali memotivasi individu untuk lebih proaktif dalam melindungi data mereka.

   c. Pendidikan dan Pelatihan

      Pendidikan mengenai keamanan siber dan pelatihan khusus tentang penggunaan smartphone yang aman memainkan peran penting dalam meningkatkan kesadaran. Kursus atau seminar yang mengajarkan cara-cara melindungi diri dari serangan siber dan mengenali tanda-tanda

serangan dapat membekali individu dengan pengetahuan yang diperlukan untuk menjaga keamanan perangkat mereka.

d. Informasi dari Media dan Sumber Terpercaya

Media, artikel, dan panduan dari sumber yang terpercaya dapat mempengaruhi kesadaran tentang ancaman keamanan. Berita terbaru tentang serangan siber, tips keamanan, dan panduan dari para ahli memberikan informasi yang sangat berguna. Paparan terhadap informasi ini secara rutin membantu pengguna tetap terinformasi dan siap menghadapi ancaman yang mungkin muncul.

e. Pengaturan dan Praktik Keamanan

Praktik keamanan yang baik, seperti mengaktifkan fitur keamanan bawaan pada smartphone, menggunakan aplikasi antivirus, dan mengelola izin aplikasi dengan bijak, merupakan indikator kesadaran yang tinggi. Pengguna yang menerapkan pengaturan ini menunjukkan kesiapan dan kepedulian dalam melindungi data pribadi mereka dari ancaman yang ada.

Kesadaran yang tinggi mengarah pada tindakan pencegahan yang lebih baik. Pengguna yang sadar akan ancaman cenderung lebih berhati-hati dalam mengunduh aplikasi, membuka email, dan mengklik link. Ini secara signifikan mengurangi risiko terkena serangan seperti malware atau phishing. Dengan memahami risiko yang ada, individu dapat melindungi informasi pribadi mereka lebih efektif. Kesadaran tentang bahaya memungkinkan pengguna untuk mengadopsi praktik keamanan yang baik, seperti penggunaan kata sandi yang kuat dan autentikasi dua faktor, yang meningkatkan perlindungan data mereka. Individu yang memiliki kesadaran tinggi tentang risiko keamanan akan lebih teliti dalam mengevaluasi izin aplikasi yang diminta dan memilih aplikasi dari sumber terpercaya. Ini membantu mereka menghindari aplikasi berbahaya yang dapat merusak perangkat atau mencuri data. Dengan melindungi perangkat dari serangan, pengguna dapat mengurangi risiko kerugian finansial akibat pencurian identitas atau kerusakan yang disebabkan oleh malware. Selain itu, melindungi reputasi pribadi dan profesional mereka juga menjadi lebih

mudah dengan menjaga keamanan data. Kesadaran yang tinggi sering kali mendorong individu untuk membagikan pengetahuan dan praktik keamanan kepada orang lain. Ini tidak hanya melindungi mereka sendiri tetapi juga membantu melindungi komunitas dari ancaman keamanan. Dengan kesadaran yang tinggi terhadap serangan pada smartphone, kita dapat melindungi diri dan data pribadi dari berbagai ancaman digital. Pengetahuan dan tindakan pencegahan yang tepat memainkan peran penting dalam menjaga keamanan perangkat dan informasi yang ada di dalamnya.

Indikator pertama mengukur kesadaran responden mengenai potensi serangan pada smartphone yang dapat mencuri data pribadi. Hasil menunjukkan bahwa 86,25% dari responden memahami risiko ini dengan baik. Persentase ini menandakan bahwa mayoritas responden menyadari bahaya serangan seperti malware dan phishing yang dapat mempengaruhi smartphone mereka. Hal ini menunjukkan tingkat pemahaman yang baik tentang bagaimana smartphone dapat menjadi target serangan dan pentingnya menjaga keamanan data pribadi.

2. Backdoor pada perangkat smartphone

Mahasiswa diharapkan menyadari bahwa beberapa smartphone mungkin sudah dilengkapi dengan backdoor pada perangkat keras atau firmware sejak dari pabrikannya. Backdoor ini dapat memungkinkan penyerang untuk mengakses data secara diam-diam tanpa sepengetahuan pengguna. Pemahaman tentang potensi keberadaan backdoor ini penting untuk memilih perangkat yang lebih aman dan melakukan tindakan pencegahan yang tepat.

Backdoor adalah pintu rahasia yang memungkinkan akses tidak sah ke perangkat kita. Ini bisa berupa kode tersembunyi dalam perangkat keras atau perangkat lunak yang memberi pihak ketiga kemampuan untuk masuk ke sistem tanpa sepengetahuan kita. Backdoor seringkali ditanam sejak pabrik, atau bisa juga disisipkan melalui modifikasi pihak ketiga. Beberapa produsen smartphone mungkin menanamkan backdoor pada perangkat mereka, baik untuk keperluan pemeliharaan atau pengumpulan data. Firmware, yang merupakan perangkat lunak dasar pada smartphone, juga

bisa mengandung backdoor yang terintegrasi sejak awal produksi. Banyak dari kita mungkin tidak menyadari adanya potensi backdoor dalam perangkat kita. Ketidaktahuan ini diperparah oleh kurangnya pemahaman mengenai risiko yang ada dan pembaruan perangkat yang terabaikan. Smartphone yang dimodifikasi oleh pihak ketiga atau aplikasi yang tidak tepercaya juga bisa menanamkan backdoor. Modifikasi atau aplikasi yang tidak resmi dapat membawa risiko tambahan yang tidak kita sadari.

Dengan backdoor, penyerang bisa mengakses data pribadi kita tanpa izin, termasuk foto, pesan, dan informasi penting lainnya. Ini bisa mengarah pada pencurian identitas dan penyalahgunaan data yang sangat merugikan. Backdoor memungkinkan pemantauan aktivitas kita secara real-time, seperti lokasi dan riwayat pencarian. Pengumpulan data tanpa persetujuan kita jelas melanggar privasi dan hak kita sebagai pengguna. Selain mencuri data, backdoor juga memungkinkan pihak ketiga untuk mengendalikan perangkat dari jarak jauh. Mereka bisa menginstal aplikasi berbahaya, mengakses kamera atau mikrofon, dan melakukan tindakan lain yang merugikan. Keberadaan backdoor dapat mengurangi keamanan sistem secara keseluruhan. Perangkat yang terinfeksi dapat menyebabkan risiko bagi jaringan yang terhubung, menyebarkan potensi ancaman ke perangkat lain.

Meningkatkan kesadaran mengenai backdoor pada smartphone sangat penting untuk melindungi data pribadi dan memastikan keamanan perangkat kita. Dengan memahami risiko ini, kita bisa lebih berhati-hati dalam memilih perangkat dan aplikasi, serta selalu memperbarui sistem keamanan untuk menjaga agar data kita tetap aman. Jangan biarkan backdoor mengancam privasi dan keamanan kita. Sub indikator kedua menilai pemahaman responden mengenai kemungkinan adanya backdoor pada smartphone yang sudah tertanam sejak pabrik. Sebanyak 86,25% responden menunjukkan kesadaran yang baik tentang keberadaan backdoor perangkat keras. Angka ini mencerminkan bahwa mereka memahami adanya risiko tambahan dari backdoor yang dapat digunakan untuk akses tidak sah dan pengumpulan data tanpa sepengetahuan pengguna.

3. Risiko dari aplikasi yang tidak resmi

Kesadaran tentang risiko penggunaan aplikasi yang tidak diunduh dari sumber resmi juga merupakan faktor krusial. Mahasiswa perlu memahami bahwa aplikasi yang diunduh dari luar Google Play Store atau repositori resmi lainnya dapat mengandung backdoor atau malware yang membahayakan keamanan data. Pengetahuan ini membantu mahasiswa dalam memilih aplikasi yang lebih terpercaya dan aman.

Kesadaran terhadap risiko aplikasi dari sumber tidak resmi merupakan aspek penting dalam menjaga keamanan informasi. Beberapa faktor yang mempengaruhi kesadaran ini antara lain pendidikan dan pengetahuan teknis, pengalaman pribadi, paparan informasi, serta persepsi risiko. Mahasiswa yang memiliki pemahaman lebih baik tentang keamanan siber cenderung lebih waspada terhadap aplikasi yang diunduh dari luar toko resmi. Selain itu, pengalaman negatif seperti terkena malware atau kebocoran data dapat meningkatkan kewaspadaan. Paparan informasi melalui kampanye kesadaran dan media sosial juga berperan penting dalam membentuk pemahaman ini. Persepsi risiko yang tinggi terhadap bahaya aplikasi dari sumber tidak resmi turut mendorong mahasiswa untuk lebih berhati-hati.

Akibat dari penggunaan aplikasi dari sumber tidak resmi dapat sangat merugikan. Infeksi malware adalah salah satu ancaman utama, di mana malware dapat merusak perangkat, mencuri data, atau bahkan mengontrol perangkat dari jarak jauh. Kebocoran data pribadi juga menjadi risiko signifikan, terutama jika aplikasi tersebut memiliki akses tanpa izin terhadap informasi sensitif. Selain itu, serangan phishing dapat terjadi melalui aplikasi tidak resmi, yang bisa menipu pengguna untuk memberikan data pribadi atau finansial. Penggunaan aplikasi ini juga dapat menyebabkan kerusakan atau performa buruk pada perangkat, serta berpotensi menimbulkan pelanggaran keamanan pada jaringan yang lebih besar. Oleh karena itu, kesadaran yang tinggi terhadap risiko ini sangat penting untuk mencegah berbagai ancaman yang dapat berdampak negatif, baik bagi individu maupun lingkungan di sekitar mereka.

Sub indikator ketiga mengukur kesadaran responden tentang risiko

aplikasi yang tidak diunduh dari Google Play Store atau repositori resmi. Dengan persentase 91,87%, responden menunjukkan pemahaman yang sangat baik tentang bahaya aplikasi dari sumber tidak resmi, termasuk potensi adanya malware atau backdoor. Persentase tinggi ini menunjukkan bahwa responden cenderung berhati-hati dalam memilih aplikasi dan memahami pentingnya mendownload aplikasi hanya dari sumber terpercaya.

4. Pertimbangan hak akses aplikasi

Selain itu, penting bagi mahasiswa untuk mempertimbangkan hak akses yang diminta oleh aplikasi sebelum menginstalnya. Memahami hak akses apa saja yang dibutuhkan aplikasi dapat membantu pengguna menilai apakah aplikasi tersebut benar-benar diperlukan dan aman untuk diinstal. Ini merupakan langkah preventif yang dapat melindungi data pribadi dari akses yang tidak sah.

Kesadaran terhadap hak akses aplikasi merupakan aspek penting dalam menjaga keamanan dan privasi data pribadi mahasiswa. Faktor-faktor yang memengaruhi kesadaran ini meliputi pemahaman terhadap privasi, di mana mahasiswa yang menyadari pentingnya melindungi data pribadi cenderung lebih selektif dalam memberikan izin akses aplikasi. Selain itu, pengalaman buruk sebelumnya, seperti data yang disalahgunakan, juga dapat meningkatkan kewaspadaan mereka. Tingkat literasi digital yang baik, didukung oleh pendidikan yang memadai tentang risiko izin aplikasi, serta sumber informasi yang tepercaya, turut berperan dalam memperkuat kesadaran ini.

Akibat dari kesadaran yang tinggi terhadap hak akses aplikasi sangat positif. Mahasiswa yang selektif dalam memberikan izin dapat melindungi data pribadi mereka dari pengumpulan yang tidak relevan dan berpotensi merugikan. Selain itu, risiko keamanan seperti malware dan pencurian data dapat diminimalisir, karena mahasiswa lebih cenderung menghindari aplikasi yang mencurigakan atau berbahaya. Kesadaran ini juga memberikan kendali yang lebih baik atas perangkat, memastikan hanya aplikasi yang tepercaya dan diperlukan yang memiliki akses ke fitur penting.

Selain itu, dengan menolak izin yang tidak relevan, penggunaan sumber daya perangkat menjadi lebih efisien, memperpanjang masa pakai baterai dan mengurangi konsumsi data serta memori. Dengan demikian, kesadaran terhadap hak akses aplikasi tidak hanya melindungi keamanan informasi, tetapi juga meningkatkan efisiensi penggunaan perangkat bagi mahasiswa. Sub indikator keempat mengevaluasi kesadaran responden mengenai pentingnya memeriksa hak akses aplikasi sebelum menginstalnya. Dengan persentase 87,18%, sebagian besar responden menunjukkan pemahaman yang baik tentang perlunya mengevaluasi hak akses aplikasi. Ini menunjukkan bahwa mereka cenderung memperhatikan izin yang diminta aplikasi dan menyadari potensi risiko yang terkait dengan izin berlebihan.

5. Sertifikasi dan keamanan perangkat

Terakhir, mahasiswa perlu menyadari bahwa smartphone yang aman untuk digunakan adalah yang telah lulus "Build Test Suite" dan memiliki sertifikasi OEM (Original Equipment Manufacturer). Sertifikasi ini menunjukkan bahwa perangkat telah menjalani uji kualitas dan keamanan, sehingga lebih andal dalam melindungi data pribadi.

Kesadaran terhadap sertifikasi keamanan smartphone dipengaruhi oleh beberapa faktor penting. Pertama, edukasi dan informasi yang diterima oleh mahasiswa sangat berperan dalam meningkatkan pemahaman mereka mengenai risiko keamanan pada perangkat yang tidak bersertifikasi. Selain itu, pengalaman pribadi atau pengalaman orang lain yang pernah mengalami masalah keamanan juga mendorong peningkatan kesadaran ini. Pengaruh media dan iklan yang menyoroti fitur keamanan pada smartphone turut berkontribusi, di samping perkembangan teknologi dan keamanan digital yang semakin kompleks.

Tingkat kesadaran yang tinggi ini membawa beberapa akibat positif. Mahasiswa cenderung memilih smartphone yang telah lulus "Build Test Suite" dan memiliki sertifikasi OEM, yang memberikan jaminan perangkat lebih aman dan terlindungi dari risiko serangan atau pencurian data. Selain itu, kesadaran ini juga meningkatkan perlindungan terhadap data pribadi karena perangkat yang bersertifikasi umumnya lebih andal dalam menjaga

keamanan. Kepercayaan terhadap produsen smartphone yang memiliki reputasi baik dalam hal keamanan juga meningkat, yang pada gilirannya memengaruhi loyalitas konsumen terhadap merek tertentu. Meski demikian, kesadaran ini juga dapat menyebabkan peningkatan biaya karena perangkat yang lebih aman biasanya memiliki harga lebih tinggi. Namun, mahasiswa umumnya melihat investasi ini sebagai langkah yang sepadan untuk mendapatkan tingkat keamanan yang lebih baik. Hasil menunjukkan bahwa 89,06% responden memahami bahwa smartphone dengan sertifikasi ini umumnya lebih aman. Persentase ini mencerminkan bahwa responden memahami pentingnya memilih perangkat yang telah melalui pengujian keamanan yang ketat dan memiliki jaminan dari produsen.

3. Tingkat Kesadaran Pengguna Akan Keamanan Informasi Dari Dimensi Sikap (*Behaviour*) Mahasiswa Prodi Ilmu Perpustakaan UIN Sumatera Utara Dalam Bersosial Media

Salah satu aspek penting yang diukur dalam menentukan tingkat kesadaran keamanan informasi mahasiswa adalah indikator behavior. Indikator ini mencakup perilaku mahasiswa dalam menghadapi risiko keamanan informasi, terutama dalam konteks penggunaan media sosial dan perangkat digital. Indikator behavior berusaha untuk mengungkap sejauh mana mahasiswa Prodi Ilmu Perpustakaan menyadari dan mengambil langkah-langkah preventif terhadap potensi ancaman keamanan yang ada.

Dalam menilai perilaku responden mengenai potensi serangan *backdoor*. Sebanyak 87,5% responden menyadari bahwa smartphone berpotensi terkena serangan berbasis *backdoor*, yang dapat memberikan akses kepada penyerang untuk mencuri data pribadi. Kesadaran ini penting karena serangan *backdoor* bisa mengakibatkan dampak serius seperti pencurian data sensitif. Hasil ini menunjukkan bahwa sebagian besar mahasiswa paham akan risiko ini dan kemungkinan besar telah mengambil langkah pencegahan yang sesuai. Selanjutnya, Sebanyak 85% responden mengetahui adanya risiko *backdoor* yang ditanamkan sejak dari pabrik oleh beberapa produsen smartphone. Meskipun sulit untuk mendeteksi *backdoor* semacam ini, kesadaran responden menunjukkan bahwa mereka menyadari risiko potensial dari perangkat yang mungkin telah

dimodifikasi untuk tujuan spionase atau aktivitas berbahaya lainnya. Hal ini mengindikasikan tingkat kehati-hatian yang baik di kalangan mahasiswa.

Lalu, dalam menilai perilaku responden mengenai risiko dari aplikasi yang tidak diunduh dari sumber resmi dimana 92,5% responden memahami bahwa penggunaan aplikasi dari luar toko resmi seperti Google Play Store dapat meningkatkan risiko serangan berbasis *backdoor*. Responden menyadari bahwa aplikasi yang tidak diverifikasi lebih rentan terhadap malware dan pencurian data, yang menandakan bahwa mereka cenderung berhati-hati dalam memilih dan menginstal aplikasi.

Selanjutnya, menilai perilaku responden mengenai pertimbangan hak akses aplikasi sebelum install, sebanyak 89,68% responden menyadari pentingnya mempertimbangkan hak akses aplikasi sebelum menginstalnya. Kesadaran ini menunjukkan pemahaman yang baik bahwa hak akses yang berlebihan dapat disalahgunakan oleh aplikasi untuk mengakses data pribadi secara tidak sah. Hal ini mencerminkan tingkat pemahaman yang baik dalam mengelola izin aplikasi.

Lalu, perilaku keamanan perangkat berdasarkan sertifikasi OEM (*Original Equipment Manufacturer*) dan proses Build Test Suite, sebanyak 89,37% responden menyadari pentingnya menggunakan perangkat yang telah lulus "Build Test Suite" dan memiliki sertifikasi OEM. Kesadaran ini menunjukkan bahwa sebagian besar mahasiswa memahami pentingnya menggunakan perangkat asli dan tersertifikasi untuk mengurangi risiko keamanan.

Sehingga dapat disimpulkan bahwa, indikator *behavior* dalam penelitian ini memperoleh persentase sebesar 88.81%, yang masuk dalam kategori baik. Hasil ini menunjukkan bahwa mahasiswa memiliki kesadaran yang tinggi terhadap beberapa aspek penting dalam keamanan informasi, seperti potensi serangan backdoor pada smartphone, risiko penggunaan smartphone yang sudah tertanam backdoor dari pabrik, bahaya mengunduh aplikasi dari sumber yang tidak resmi, pentingnya mempertimbangkan hak akses aplikasi sebelum instalasi, serta pentingnya keamanan perangkat yang telah memperoleh sertifikasi OEM dan lulus pengujian Build Test Suite.

Selanjutnya masing-masing sub indikator akan dipaparkan dalam poin-poin berikut:

1. Potensi serangan backdoor pada smartphone

Pada sub indikator ini, terdapat beberapa faktor dan akibat yang perlu diperhatikan. Faktor utama yang meningkatkan risiko serangan backdoor adalah kecerobohan pengguna dalam mengelola aplikasi. Banyak pengguna smartphone yang tidak menyadari bahwa aplikasi yang mereka unduh, terutama dari sumber yang tidak resmi, bisa mengandung backdoor yang membahayakan. Kurangnya pengetahuan tentang keamanan digital juga berperan penting, karena banyak pengguna yang belum sepenuhnya memahami konsep backdoor dan cara kerjanya. Selain itu, penggunaan perangkat yang tidak tersertifikasi dapat meningkatkan risiko, karena perangkat semacam ini seringkali tidak memiliki perlindungan yang memadai terhadap eksploitasi.

Akibat dari serangan backdoor bisa sangat merugikan. Salah satu akibat utama adalah pencurian data pribadi, di mana penyerang dapat mengakses kontak, pesan, foto, dan informasi finansial pengguna tanpa sepengetahuan mereka. Hal ini dapat berujung pada pencurian identitas atau penyalahgunaan data untuk tujuan ilegal. Selain itu, penyerang yang memanfaatkan backdoor dapat mengontrol perangkat korban dari jarak jauh, menginstal malware, atau menggunakan perangkat tersebut untuk melakukan serangan siber lainnya. Dampak lain yang signifikan adalah kerugian finansial dan reputasi. Jika data yang dicuri mencakup informasi finansial, pengguna bisa mengalami kerugian materi. Selain itu, pencurian atau penyalahgunaan data juga dapat merusak reputasi pribadi pengguna, terutama jika informasi tersebut dipublikasikan atau digunakan untuk aktivitas yang tidak sah. Faktor-faktor ini menunjukkan pentingnya peningkatan kesadaran pengguna tentang risiko keamanan informasi serta perlunya langkah-langkah proaktif untuk melindungi perangkat mereka dari potensi serangan backdoor.Sebanyak 87,5% responden menyadari bahwa smartphone berpotensi terkena serangan berbasis backdoor, yang dapat memberikan akses kepada penyerang untuk mencuri data pribadi. Kesadaran ini penting karena serangan backdoor bisa mengakibatkan dampak serius seperti pencurian data sensitif. Hasil ini menunjukkan bahwa

sebagian besar mahasiswa paham akan risiko ini dan kemungkinan besar telah mengambil langkah pencegahan yang sesuai.

2. Smartphone sudah tertanan backdoor

Backdoor perangkat keras pada firmware dari pabrik dapat timbul dari beberapa faktor. Salah satunya adalah motivasi produsen yang mungkin menanamkan backdoor untuk tujuan spionase atau pengumpulan data pengguna secara massal. Data yang terkumpul dari backdoor ini dapat digunakan untuk analisis pasar atau bahkan dijual kepada pihak ketiga. Selain itu, backdoor mungkin digunakan untuk tujuan keamanan internal, seperti pemantauan perangkat yang hilang, meskipun hal ini dapat menimbulkan risiko jika akses tidak dikelola dengan baik. Keterbatasan regulasi dan pengawasan juga berperan, di mana regulasi yang lemah memungkinkan produsen untuk menyematkan backdoor tanpa terdeteksi.

Akibat dari adanya backdoor dalam firmware sangat beragam dan serius. Salah satunya adalah risiko pencurian data pribadi, di mana penyerang dapat mengakses informasi sensitif pengguna seperti kontak, pesan, dan data penting lainnya, yang berpotensi mengakibatkan kerugian privasi dan finansial. Backdoor juga meningkatkan kerentanan terhadap serangan siber lebih lanjut, karena pihak ketiga dapat memanfaatkan akses ini untuk melakukan tindakan berbahaya. Selain itu, backdoor dapat mempengaruhi kinerja perangkat, menyebabkan perangkat menjadi lambat atau tidak responsif. Dampak lainnya adalah penurunan kepercayaan pengguna terhadap produsen perangkat, karena penemuan backdoor dapat merusak reputasi merek dan menimbulkan kekhawatiran tentang integritas perangkat. Kesulitan dalam deteksi backdoor yang tersembunyi dalam firmware membuatnya semakin sulit untuk diidentifikasi dan diatasi oleh pengguna atau profesional keamanan, menambah kompleksitas masalah ini.

Sebanyak 85% responden mengetahui adanya risiko backdoor yang ditanamkan sejak dari pabrik oleh beberapa produsen smartphone. Meskipun sulit untuk mendeteksi backdoor semacam ini, kesadaran responden menunjukkan bahwa mereka menyadari risiko potensial dari perangkat yang mungkin telah dimodifikasi untuk tujuan spionase atau

aktivitas berbahaya lainnya. Hal ini mengindikasikan tingkat kehati-hatian yang baik di kalangan mahasiswa.

3. Risiko dari aplikasi yang tidak diunduh dari sumber resmi

Mengunduh aplikasi dari sumber non-resmi dapat menimbulkan berbagai risiko yang serius. Salah satu faktor utama adalah kurangnya verifikasi keamanan. Aplikasi yang diunduh dari sumber tidak terpercaya tidak melalui proses verifikasi ketat seperti yang diterapkan oleh toko aplikasi resmi seperti Google Play Store atau Apple App Store. Tanpa verifikasi ini, aplikasi tersebut lebih rentan terhadap infeksi malware. Selain itu, aplikasi dari sumber non-resmi sering kali tidak memenuhi standar pengembangan yang sama dengan aplikasi dari toko resmi, yang dapat mengakibatkan kurangnya pembaruan dan perbaikan bug yang meningkatkan risiko keamanan. Malware, termasuk virus dan trojan, sering kali disamarkan sebagai aplikasi sah, sehingga sulit dikenali dan dihindari.

Akibat dari mengunduh aplikasi dari sumber non-resmi bisa sangat merugikan. Salah satu akibat utama adalah infeksi malware, yang dapat merusak sistem perangkat, memperlambat kinerja, atau bahkan menyebabkan perangkat tidak berfungsi dengan baik. Malware juga dapat menyebar ke perangkat lain yang terhubung. Selain itu, pencurian data pribadi adalah risiko besar, di mana aplikasi tidak terpercaya dapat mengakses dan mencuri informasi sensitif seperti kontak, foto, dan data keuangan. Data yang dicuri bisa digunakan untuk penipuan atau dijual di pasar gelap, menyebabkan kerusakan reputasi dan privasi bagi individu. Terakhir, aplikasi yang mengandung malware atau tidak berfungsi dengan baik dapat mengakibatkan penurunan kinerja perangkat, termasuk crash atau kerusakan sistem. Oleh karena itu, sangat penting bagi pengguna untuk berhati-hati dalam memilih sumber unduhan aplikasi untuk melindungi perangkat dan data pribadi mereka dari risiko yang tidak diinginkan.Kesadaran tertinggi ditunjukkan pada item ini, di mana 92,5% responden memahami bahwa penggunaan aplikasi dari luar toko resmi seperti Google Play Store dapat meningkatkan risiko serangan berbasis backdoor. Responden menyadari bahwa aplikasi yang tidak diverifikasi

lebih rentan terhadap malware dan pencurian data, yang menandakan bahwa mereka cenderung berhati-hati dalam memilih dan menginstal aplikasi.

4. Pertimbangan hak akses aplikasi sebelum install

Pertimbangan hak akses aplikasi sebelum menginstal merupakan langkah penting dalam menjaga keamanan informasi dan data pribadi. Salah satu faktor utama yang mempengaruhi perilaku ini adalah kesadaran mahasiswa mengenai jenis dan jumlah hak akses yang diminta oleh aplikasi. Mahasiswa yang memiliki pemahaman mendalam tentang fungsi aplikasi dan relevansi hak akses yang diminta cenderung lebih berhati-hati dalam memberikan izin. Pengetahuan tentang risiko keamanan yang terkait dengan hak akses berlebihan juga berperan besar, dengan mahasiswa yang lebih paham risiko tersebut akan lebih teliti dalam memeriksa izin yang diminta sebelum instalasi. Selain itu, pengalaman pribadi dengan aplikasi yang pernah menimbulkan masalah keamanan atau informasi dari sumber terpercaya dapat mempengaruhi sikap mahasiswa. Program edukasi atau penyuluhan mengenai keamanan informasi yang disediakan di kampus atau melalui media sosial juga berkontribusi dalam membentuk perilaku ini.

Dengan mempertimbangkan hak akses aplikasi, mahasiswa dapat mengurangi risiko pencurian data pribadi dan mencegah perangkat mereka dari infeksi malware atau serangan siber. Proses ini juga meningkatkan kesadaran keseluruhan tentang keamanan siber, menjadikan mahasiswa lebih proaktif dalam melindungi data pribadi mereka. Namun, perlu dicatat bahwa menolak hak akses yang dianggap tidak relevan bisa berdampak pada fungsi aplikasi, di mana beberapa aplikasi mungkin memerlukan akses tertentu untuk berfungsi dengan baik. Secara keseluruhan, evaluasi hak akses aplikasi adalah langkah kritis dalam melindungi informasi pribadi dan mengurangi risiko yang terkait dengan penggunaan aplikasi digital.Sebanyak 89,68% responden menyadari pentingnya mempertimbangkan hak akses aplikasi sebelum menginstalnya. Kesadaran ini menunjukkan pemahaman yang baik bahwa hak akses yang berlebihan dapat disalahgunakan oleh aplikasi untuk mengakses data pribadi secara tidak sah. Hal ini mencerminkan tingkat pemahaman yang baik dalam

mengelola izin aplikasi.

5. Keamanan perangkat berdasarkan sertifikasi dan pengujian

   Faktor utama yang berkontribusi pada keamanan perangkat adalah sertifikasi OEM (Original Equipment Manufacturer) dan proses Build Test Suite. Sertifikasi OEM menunjukkan bahwa perangkat adalah produk asli dari produsennya dan telah menjalani proses pengujian yang ketat, menjamin bahwa perangkat memenuhi standar kualitas dan keamanan tertentu. Selain itu, Build Test Suite mencakup serangkaian tes yang dirancang untuk memastikan perangkat berfungsi dengan baik dan bebas dari kerentanan keamanan yang dapat dimanfaatkan oleh penyerang.

Akibat dari penggunaan perangkat yang telah tersertifikasi dan lulus uji kualitas ini sangat signifikan. Pertama, risiko infeksi malware dan serangan siber berkurang secara drastis karena proses pengujian memastikan bahwa perangkat tidak memiliki kerentanan yang dapat dieksploitasi. Kedua, sertifikasi dan pengujian meningkatkan kepercayaan konsumen terhadap perangkat yang mereka beli, memberikan jaminan bahwa perangkat tersebut aman dan berkualitas. Selanjutnya, perlindungan terhadap data pribadi juga lebih terjamin, karena perangkat yang telah teruji tidak mengandung backdoor atau kerentanan lain yang dapat digunakan untuk mencuri informasi. Terakhir, perangkat yang telah melewati pengujian yang ketat cenderung mengalami lebih sedikit masalah teknis, mengurangi kebutuhan untuk perbaikan dan dukungan teknis, serta menghemat biaya dan waktu bagi pengguna. Dengan demikian, sertifikasi dan pengujian perangkat memainkan peran penting dalam meningkatkan keamanan dan kualitas, serta memberikan perlindungan yang lebih baik terhadap data pribadi pengguna. Sebanyak 89,37% responden menyadari pentingnya menggunakan perangkat yang telah lulus "Build Test Suite" dan memiliki sertifikasi OEM. Kesadaran ini menunjukkan bahwa sebagian besar mahasiswa memahami pentingnya menggunakan perangkat asli dan tersertifikasi untuk mengurangi risiko keamanan

Berdasarkan hasil penelitian yang menunjukkan bahwa indikator *attitude*, *knowledge*, dan *behavior* mahasiswa Prodi Ilmu Perpustakaan Stambuk 2020-2021 Universitas Islam Negeri Sumatera Utara dalam bersosial media berada

dalam kategori baik dengan persentase rata-rata sebesar 88,82%, terdapat beberapa faktor utama yang berkontribusi terhadap hasil ini. Pertama, tingkat pengetahuan atau *knowledge* yang memadai tentang keamanan informasi menjadi salah satu faktor penentu. Mahasiswa memiliki pemahaman yang baik mengenai pentingnya melindungi data pribadi dan menyadari risiko yang mungkin timbul jika data mereka tidak aman. Pengetahuan ini mendorong mereka untuk menerapkan langkah-langkah keamanan yang diperlukan, seperti menggunakan enkripsi, mengaktifkan autentikasi dua faktor, dan mengelola izin akses data dengan bijaksana.

Kedua, sikap atau *attitude* mahasiswa terhadap keamanan informasi juga menunjukkan respons positif. Mahasiswa menunjukkan kepedulian yang tinggi terhadap keamanan data mereka, baik dalam menjaga data yang diinput agar tidak diakses oleh pihak yang tidak berhak maupun dalam memastikan sistem yang mereka gunakan memiliki mekanisme backup yang andal. Sikap positif ini mendorong mereka untuk secara aktif menerapkan praktik-praktik terbaik dalam menjaga keamanan informasi.

Ketiga, perilaku atau *behavior* mahasiswa dalam mengelola data pribadi juga menjadi faktor kunci. Mahasiswa secara rutin menerapkan langkah-langkah pencegahan, seperti melakukan backup data secara berkala, menghindari penggunaan aplikasi dari sumber yang tidak resmi, dan memilih perangkat yang telah tersertifikasi keamanan. Perilaku yang proaktif ini mencerminkan tingkat kesadaran yang tinggi terhadap pentingnya menjaga integritas dan keamanan informasi dalam lingkungan digital. Seperti yang dipaparkan oleh Taufiq Ramadhan (Ramadhan, 2023), aplikasi kerap menjadi jalan masuk upaya *social engineering* dengan memanfaatkan kelengahan pengguna yang menginstall aplikasi dari sumber tidak resmi atau tidak terpercaya. Contoh kasus telah terjadi adalah seorang nasabah membuka aplikasi perbankan digital yang ternyata diketahui invalid hingga kemudian mengalami sejumlah kerugian materil.

Gabungan dari ketiga indikator ini yaitu pengetahuan yang memadai, sikap yang positif, dan perilaku yang proaktif berkontribusi secara signifikan terhadap capaian rata-rata persentase 88.82% pada indikator attitude,

knowledge, dan behavior, yang berada dalam kategori baik. Hal ini menunjukkan bahwa mahasiswa memiliki kesadaran yang kuat akan pentingnya keamanan informasi dalam bersosial media, serta mampu menerapkan langkah-langkah perlindungan yang efektif untuk menjaga data pribadi mereka.

Berdasarkan penelitian yang dilakukan Yoyon Arie (Arie Budi Suprio & Najib, 2022), Keamanan informasi merupakan upaya yang digunakan untuk mengamankan asset informasi data terhadap ancaman yang mungkin muncul. Kesadaran keamanan informasi merupahan hal yang penting untuk mewujudkan keamanan informasi, untuk meningkatkan kesadaran keamanan informasi bisa mengikuti berbagai kegiatan seperti pelatihan, webinar, talkshow, training, atau sharing knowledge. Berdasarkan data yang diperoleh dalam penelitian yang dilakukannya, dapat disimpulkan bahwa dampak atau pengaruh dari kesadaran keamanan informasi sangatlah penting. Dengan kemajuan teknologi yang semakin pesat, pengguna media sosial seperti whatsapp juga harus bisa menyeimbangkan dengan pengetahuanpengetahuan dasar tentang keamanan informasi

Dalam konteks penelitian yang dilakukan terhadap mahasiswa Prodi Ilmu Perpustakaan Stambuk 2021-2022 Universitas Islam Negeri Sumatera Utara, pengaruh tingkat kesadaran terhadap keamanan informasi menjadi semakin relevan mengingat peran penting yang dimiliki mahasiswa dalam mengakses dan mengelola informasi, baik untuk keperluan akademis maupun pribadi. Sebagai calon pustakawan dan profesional informasi, mahasiswa Prodi Ilmu Perpustakaan diharapkan memiliki pemahaman yang mendalam tentang pentingnya keamanan informasi, termasuk dalam penggunaan media sosial.

Tingkat kesadaran yang tinggi di kalangan mahasiswa ini sangat berpengaruh terhadap bagaimana mereka menjaga dan mengelola informasi yang mereka bagikan dan konsumsi di media sosial. Kesadaran yang baik mendorong mereka untuk lebih selektif dalam menerima informasi, lebih berhati-hati dalam membagikan data pribadi, dan lebih kritis terhadap sumber-sumber informasi yang tidak terpercaya. Hal ini penting karena media sosial sering kali menjadi sarana utama bagi mahasiswa dalam berkomunikasi,

berbagi pengetahuan, dan mengembangkan jaringan akademis.

Faktor-faktor seperti pengetahuan yang memadai tentang risiko keamanan informasi, pengalaman pribadi terkait insiden keamanan, serta sikap terhadap pentingnya melindungi data, semuanya memengaruhi tingkat kesadaran mahasiswa ini. Akses terhadap edukasi yang relevan, baik melalui kurikulum akademis maupun program-program kesadaran digital, juga sangat berperan dalam meningkatkan kesadaran mereka. Selain itu, pengaruh sosial dari rekan sejawat dan komunitas online turut membentuk sikap mereka terhadap keamanan informasi.

Secara keseluruhan, tingkat kesadaran yang baik akan menghasilkan perilaku yang lebih bertanggung jawab dan proaktif dalam menggunakan media sosial. Mahasiswa Prodi Ilmu Perpustakaan UIN Sumatera Utara yang memiliki kesadaran tinggi cenderung lebih mampu melindungi diri mereka dari ancaman keamanan informasi, menjaga integritas akademis, serta berkontribusi pada lingkungan digital yang lebih aman dan terpercaya. Sebaliknya, rendahnya kesadaran akan meningkatkan risiko terjadinya insiden keamanan informasi yang dapat berdampak buruk tidak hanya pada individu tetapi juga pada komunitas akademik secara keseluruhan

Adapun implikasi penelitian ini berdasarkan aspek sosial, agama, dan Prodi Ilmu Perpustakaan dipaparkan sebagai berikut:

1. Aspek Sosial

Penelitian ini menunjukkan pentingnya peningkatan kesadaran akan keamanan informasi dalam kehidupan sehari-hari mahasiswa. Dalam konteks sosial, mahasiswa yang lebih sadar terhadap risiko keamanan informasi cenderung lebih berhati-hati dalam berbagi informasi pribadi dan akademis di media sosial. Hal ini dapat mengurangi potensi penyebaran informasi yang tidak diinginkan atau penyalahgunaan data pribadi. Implikasi ini menekankan perlunya kampanye edukasi dan program literasi digital yang menargetkan mahasiswa untuk mengajarkan praktik keamanan informasi yang baik dan bertanggung jawab dalam interaksi sosial online.

2. Aspek Agama

Dalam konteks agama, kesadaran akan keamanan informasi juga berkaitan dengan tanggung jawab moral dan etika dalam bersosial media. Mahasiswa yang memiliki pemahaman yang baik tentang keamanan informasi akan lebih mungkin menjaga amanah dalam menyebarkan informasi yang benar dan menghindari penyebaran hoaks atau informasi yang dapat merugikan orang lain. Dari sudut pandang Islam, menjaga kerahasiaan dan integritas informasi adalah bagian dari menjaga kehormatan dan harga diri seseorang. Penelitian ini mengimplikasikan pentingnya integrasi nilai-nilai agama dalam pendidikan literasi digital, sehingga mahasiswa dapat melihat keamanan informasi sebagai bagian dari tanggung jawab keagamaan mereka.

3. Aspek Prodi Ilmu Perpustakaan

Sebagai mahasiswa Prodi Ilmu Perpustakaan, kesadaran akan keamanan informasi sangat relevan dengan disiplin ilmu mereka yang berfokus pada pengelolaan informasi. Penelitian ini mengimplikasikan bahwa peningkatan kesadaran keamanan informasi akan memberikan dampak positif terhadap kompetensi profesional mereka di masa depan. Mahasiswa yang terlatih dalam praktik keamanan informasi akan lebih siap untuk menghadapi tantangan dalam mengelola, menyimpan, dan mendistribusikan informasi secara aman dan efisien di dunia kerja. Hal ini juga mendorong Prodi Ilmu Perpustakaan untuk mengintegrasikan modul keamanan informasi dalam kurikulum mereka, guna mempersiapkan mahasiswa menghadapi tantangan keamanan di era digital.

F. Keterbatasan Penelitian

Penelitian ini hanya berfokus untuk mengukur tingkat kesadaran akan keamanan informasi mahasiswa dalam bersosial media. Sehingga persoalan mengenai bagaimana mahasiswa menjaga atau melindungi keamanan informasinya akan dilakukan penelitian lainnya. Sehingga penelitian ini memberikan referensi awal untuk dilakukan penelitian selanjutnya.

.