
PENGUKURAN KESADARAN KEAMANAN INFORMASI DAN PRIVASI PADA PENGGUNA ANDROID DI KOTA BANDUNG

Arvand Alfarizki Pratama¹⁾, Irfan Muhammad Ghufro²⁾, Jauhar ma'ruf³⁾, Sarifudin Hanafi⁴⁾, Abdul Hafidh Anas⁵⁾

email: Arvand.rizki01@gmail.com¹⁾, irfanghufro240@gmail.com²⁾, jauhar.maruf01@gmail.com³⁾, 17180051@ars.ac.id⁴⁾, abdulhafidannas99@gmail.com⁵⁾

Abstrak

Android merupakan smartphone terpopuler dengan pengguna yang mencapai 1,8 miliar pengguna di dunia. Tingginya jumlah pengguna juga memunculkan banyaknya kasus keamanan informasi dan privasi yang dikarenakan oleh kurangnya kesadaran dari pengguna seperti spam, spoofing/phising, network incident, malware, mengunggah data yang bersifat pribadi seperti foto, nomor telepon, alamat atau tidak memiliki antivirus. Penelitian ini bertujuan untuk mengetahui tentang keamanan informasi dan privasi pengguna smartphone Android di kota Bandung dengan melakukan pengukuran masalah dari dimensi kesadaran (attitude, knowledge dan behaviour) dengan tujuh fokus area keamanan informasi yaitu trust in app repository, misconception about app testing, security and agreement message, pirated application, adoption security control, spam sms dan report of security incidents dan tiga fokus area privasi yaitu perceived surveillance, perceived intrusion, secondary use of information. Jenis penelitian yang digunakan adalah metode kuantitatif dimana data yang dikumpulkan dengan menggunakan kuesioner. Secara keseluruhan, hasil dari penelitian menunjukkan bahwa keamanan informasi memiliki tingkat kesadaran rata-rata (80%). Namun pada fokus area report for security incidents memiliki tingkat kesadaran (70%) dan pada fokus privasi memiliki tingkat kesadaran rata-rata (80%). Berdasarkan hasil dari penelitian tersebut, dapat disimpulkan bahwa pengguna smartphone di kota Bandung memiliki tingkat kesadaran yang baik dalam menjaga keamanan informasi dan privasinya.

Kata Kunci: android, keamanan, smartphone.

1. Pendahuluan

Teknologi pada masa ini terus berkembang dengan pesat salah satu dari teknologi itu yaitu smartphone. Semua orang pasti tahu apa itu smartphone karena sekarang itu merupakan kebutuhan paling penting, baik untuk usaha, kerja, ataupun pendidikan. Smartphone memiliki 2 tipe sistem operasi yaitu Ios dan android. Untuk Ios dimiliki oleh perusahaan apple sedangkan Android oleh google (Ngafifi, 2014). Jumlah pengguna ios di indonesia sendiri menurut Mobile Operating System Market Share indonesia hanya sebesar 8.15% dari seluruh pengguna smartphone dengan berarti di indonesia lebih banyak pengguna android sebesar 91.61%. Alasan kenapa android banyak digunakan di indonesia karena harga yang terjangkau dan mudah digunakan.

Pengguna smartphone di indonesia cukup besar dengan berarti tingkat penggunaan internet juga merupakan salah satu yang terbesar di dunia laporan perusahaan media asal Inggris, We Are Social mengungkapkan laporan "Digital 2021: The Latest Insights Into The State of Digital" yang diterbitkan pada 11 Februari 2021. Laporan tersebut berisi hasil riset mengenai pola pemakaian media sosial dan internet di sejumlah negara termasuk di Indonesia. Dari total populasi Indonesia sebanyak 274,9 juta jiwa, pengguna aktif media sosialnya mencapai 170 juta. Jumlah pengguna media sosial di Indonesia sama dengan 61,8 persen dari total populasi pada Januari 2021. Angka ini juga meningkat 10 juta, atau sekitar 6,3 persen dibandingkan tahun lalu (Rizal, 2021). Tingginya jumlah tersebut mengundang banyak bahaya yang berhubungan dengan privasi dan informasi pengguna.

Tujuan dari penelitian ini adalah untuk mengetahui tingkat kesadaran masyarakat indonesia tentang pemahaman menjaga privasi dan informasi dalam penggunaan smartphone dengan mengetahui itu diharapkan banyak masyarakat yang akan sadar akan pentingnya menjaga data-data informasi mereka di smartphone sehingga tingkat kejahatan pencurian data bisa dikurangi.

Sebelum proses pemodelan, dilakukan juga *pre-processing* data dengan menggunakan teknik *resampling*, yaitu salah satu teknik *pre-processing* untuk menyeimbangkan distribusi data sehingga mengurangi efek distribusi kelas atau kategori yang tidak seimbang (Jian et al. 2016). [8] Ketidakseimbangan data memberikan dampak yang buruk pada hasil klasifikasi dimana kelas minoritas sering disalahklasifikasikan sebagai kelas mayoritas.

Proses *resampling* dilakukan karena data lansia yang merokok jauh lebih kecil dibandingkan data lansia yang masih merokok. Data sampel penduduk lanjut usia yang diperoleh terdiri dari sekitar 11 persen lansia Indonesia berhenti merokok tembakau sedangkan sisanya masih merokok. Teknik *resampling* yang digunakan adalah *random oversampling* dan *random undersampling*. *Random oversampling* digunakan untuk menyeimbangkan

data dengan cara *oversampling* secara acak pada kelas minoritas (penduduk lansia yang berhenti merokok). *Random undersampling* digunakan untuk menyeimbangkan data dengan cara *undersampling* (mengeliminasi) secara acak kelas mayoritas (penduduk lansia yang masih merokok)

Tujuan dari penelitian ini: (1) mengetahui karakteristik penduduk lanjut usia (lansia) yang berhenti merokok; (2) mengaplikasikan metode regresi logistik biner untuk mengidentifikasi faktor apa saja yang menjadi determinan berhenti merokok lansia; (3) menentukan metode regresi logistik biner dengan proses *resampling* (*undersampling* dan *oversampling*) atau metode regresi logistik biner tanpa proses *resampling* yang merupakan model terbaik dalam mengklasifikasikan lansia yang berhenti merokok.

2. Landasan Teori

Keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi. (Witman, 2011). Menurut Melwin Syafrizal keamanan informasi terbagi menjadi tiga perlindungan terhadap aspek-aspek yaitu Confidentiality (kerahasiaan) yang menjamin kerahasiaan data atau informasi, Integrity (integritas) suatu aspek yang menjamin data tidak bisa diubah tanpa ijin, dan Availability (ketersediaan) yang menjamin bahwa data akan selalu tersedia saat dibutuhkan. (Syafrizal, 2007).

Menurut Xu et al., persepsi pengguna smartphone dari sudut pandang pengawasan terhadap pengguna bisa sangat menonjol karena kegiatan pengumpulan data yang agresif oleh aplikasi mobile. Kedua, persepsi intrusi dapat dipicu ketika aturan kepemilikan dilanggar, yaitu, ketika aplikasi mobile mampu membuat keputusan independen tentang memiliki atau meminta informasi pribadi pengguna. Dalam penelitian ini dan berdasarkan penelitian sebelumnya privasi terdiri dari tiga indikator yaitu perceived surveillance, perceived intrusion, secondary use information. (Xu & Rosson, 2012).

Menurut Whitman dan Mattord, security Awareness adalah kontrol/aturan yang dirancang untuk mengurangi insiden pelanggaran terhadap keamanan informasi, akibat dari kelalaian maupun tindakan yang telah direncanakan. Menurut Kruger & Kerney, menggunakan teori psikologi sosial membagi tiga komponen untuk mengukur objek yakni cognition, affection dan behaviour. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai Knowledge (pengetahuan seseorang), Attitude (sikap seseorang) dan Behaviour (perilaku seseorang). (Kruger & W.D, 2006)

3. Metode Penelitian

Jenis penelitian yang digunakan adalah metode kuantitatif dimana data yang dikumpulkan dengan menggunakan kuesioner. Penelitian ini memiliki 5 pertanyaan dari kesadaran keamanan informasi dan 5 pertanyaan dari kesadaran privasi untuk menguji attitude, knowledge dan behavior dalam perspektif penggunaan *smartphone Android*. Contoh pertanyaan yang diajukan dapat dilihat di Tabel 0.1. Kuesioner disebar secara online.

Tabel 1. Contoh pertanyaan

Tabel 1. Pertanyaan

| Dimensi | Pertanyaan |
|--|--|
| Tingkat kesadaran keamanan dan informasi | Data yang anda input aman dari orang yang tidak berhak mengakses |
| | Sistem mempunyai backup data yang bagus |
| | Data anda tidak hilang meskipun listrik mati mendadak |
| | Data anda tidak hilang meskipun smartphone anda rusak |
| | Sistem informasi jarang crash |
| Attitude | Saya sadar bahwa smartphone berbasis android mendapatkan serangan yang dapat memberikan akses kepada penyerang untuk mencuri data informasi pribadi |
| | Saya sadar bahwa beberapa smartphone Android tertentu sudah tertanam atau diselipkan backdoor perangkat keras pada firmware sejak dari pabrikannya |
| | Saya sadar bahwa penggunaan aplikasi tidak diunduh dari google play store atau repositori resmi dapat meningkatkan resiko serangan berbasis backdoor |
| | Saya sadar untuk mempertimbangkan hak akses apa saja yang dibutuhkan suatu aplikasi sebelum meng-instalnya (termasuk dari Google Play Store atau repositori resmi lainnya) |
| | Saya sadar bahwa smartphone yang aman digunakan adalah yang telah lulus "Build Test Suite" dan telah mempunyai sertifikasi OEM (Original Equipment Manufacture) atau juga bisa disebut barang original |

| | |
|-----------|--|
| Knowledge | Smartphone berbasis Android berpotensi mendapatkan serangan berbasis backdoor yang dapat memberikan akses kepada penyerang untuk mencuri data informasi pribadi pengguna |
| | Beberapa smartphone Android tertentu sudah tertanam atau diselipkan backdoor perangkat keras pada firmware sejak dari pabrikannya |
| | Penggunaan aplikasi yang tidak diunduh dari Google Play Store atau repositori resmi lainnya dapat meningkatkan risiko serangan berbasis backdoor |
| | Sebelum install suatu aplikasi (termasuk dari Google Play Store atau repositori resmi lainnya), perlu dipertimbangkan hak akses apa saja yang dibutuhkan untuk berjalan |
| | Smartphone yang aman digunakan adalah yang telah lulus "Build Test Suite" dan telah mempunyai sertifikasi OEM atau "Original Equipment Manufacture" atau juga bisa disebut barang original |
| Behavior | Saya terbiasa untuk melakukan langkah-langkah pencegahan atas serangan berbasis backdoor di smartphone Android saya |
| | Saya terbiasa untuk tidak menggunakan smartphone Android tertentu yang berpotensi telah tertanam atau diselipkan backdoor perangkat keras pada firmware sejak dari pabrikannya. |
| | Saya terbiasa untuk tidak menggunakan aplikasi yang tidak diunduh dari Google Play Store atau repositori resmi lainnya |
| | Saya terbiasa melakukan pertimbangan hak akses apa saja yang dibutuhkan suatu aplikasi sebelum meng-instalnya, termasuk dari Google play Store atau repositori resmi lainnya |
| | Saya terbiasa untuk hanya menggunakan smartphone Android yang telah lulus "Build Test Suite" dan telah mempunyai sertifikasi OEM (Original Equipment Manufacture) atau juga bisa disebut barang original |

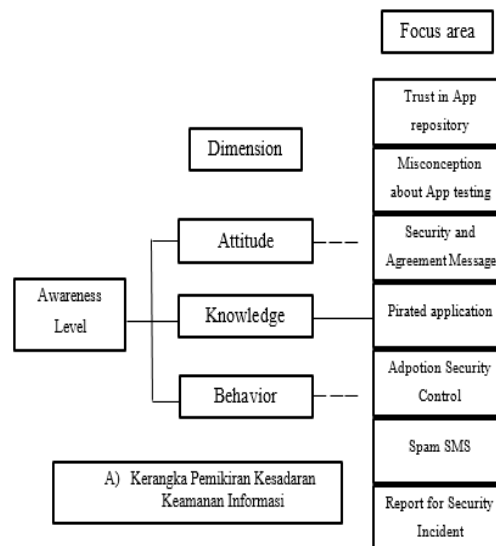
Variabel operasional dalam penelitian ini terdiri dari tiga dimensi, yaitu pengetahuan (apa yang mereka ketahui tentang keamanan dan privasi), Sikap (bagaimana perasaan mereka tentang keamanan dan privasi), Dan perilaku (apa yang mereka lakukan terhadap keamanan dan privasi) Masing-masing dimensi tersebut kemudian terbagi menjadi tujuh fokus area keamanan informasi yaitu *trust in application repository*, *misconception about app testing*, *Security and agreement message*, *pirated applicaion*, *adoption of security control* spam sms dan *report of security incidents*. dan tiga fokus area privasi yaitu *perceived surveillance*, *perceived intrusion* dan *secondary use information*.

(Sari, 2014) mengatakan bahwa pembobotan ditentukan dengan menggunakan *analytical hierarchy process* (AHP). Setiap dimensi memiliki bobot yang akan digunakan dalam perhitungan skor kesadaran. Bobot tersebut didefinisikan pada Tabel 0.2. sebagai berikut. Bobot tersebut didefinisikan pada Tabel 2. sebagai berikut.

Tabel 2. Bobot

| Dimensi | Bobot |
|------------------|-------|
| <i>Attitude</i> | 20 |
| <i>Knowledge</i> | 30 |
| <i>Behaviour</i> | 50 |

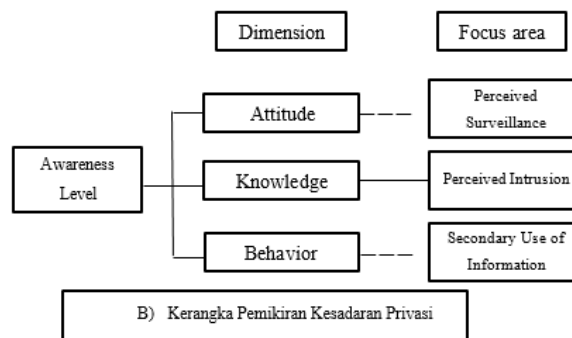
Kerangka pemikiran dari penelitian ini menggunakan model Krueger dan Kerney (2006) yang mengadaptasi teori psikologi sosial yang mengusulkan tiga komponen untuk mengukur cara yang menguntungkan atau tidak menguntungkan terhadap objek tertentu. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai *knowledge* (pengetahuan seseorang), *attitude* (sikap seseorang) dan *behaviour* (perilaku seseorang). Dimensi *knowledge* digunakan untuk mengetahui bagaimana pengetahuan pengguna. Sedangkan Dimensi *attitude* digunakan untuk mengetahui bagaimana sikap pengguna dan dimensi *behaviour* untuk mengetahui hal-hal yang dapat dilakukan oleh pengguna. Masing-masing dimensi tersebut kemudian terbagi menjadi tujuh fokus area keamanan informasi dan tiga fokus area privasi. Berikut ini adalah metode yang diadopsi dari model Kruger dan Kearney seperti yang ditunjukkan pada Gambar 0.1



Gambar 0.1 Kerangka Pemikiran Kesadaran Keamanan Informasi

Kerangka pemikiran dari penelitian ini menggunakan model Hennie A Krueger dan W.D Kearney (2006) untuk mengukur tingkat kesadaran dari tiap-tiap fokus area yang lima diantaranya diadaptasi dari (Mylonas & Gritzalis, 2013) yaitu *trust in app repository*, *misconception about app testing*, *security and agreement message*, *pirated application*, dan *adoption of security control* dimana *trust in app repository* bisa dilihat dari rasa percaya pengguna smartphone untuk mengunduh aplikasi di toko aplikasi atau *repository* aplikasi yang sudah disediakan oleh sistem operasi dari *smartphone* yang digunakan.

Adapun dua fokus area lainnya dari kerangka pemikiran kesadaran keamanan informasi pada Gambar 1 yang diadaptasi dari Sari et al. (2014) yaitu *spam sms* dan *report for security incident*. Ketujuh fokus area yang telah disebutkan di atas, digabungkan bertujuan agar penelitian lebih komprehensif untuk mengukur kesadaran keamanan informasi. Sedangkan kerangka pemikiran kesadaran privasi dapat dilihat pada Gambar 0.2



Gambar 0.2 Kerangka Pemikiran Kesadaran Privasi

Pada Gambar 2, kerangka pemikiran kesadaran privasi juga di adaptasi dari model Krueger dan Kerney (2006) dan fokus areaya diadaptasi dari Xu et al. (2012) yang menggunakan *perceived surveillance*, *perceived intrusion*, dan *secondary use of information* untuk mengukur kesadaran privasi pengguna smartphone. Pengukuran kesadaran privasi ini perlu dilakukan untuk mengetahui sejauh mana pengguna dapat mengendalikan informasi pribadi pengguna terhadap hak akses yang diminta oleh aplikasi mobile dan kekhawatiran penyalahgunaan informasi oleh pengembang aplikasi dan pihak ketiga.

4. Hasil Penelitian

Hasil dari data survey yang telah di kirim secara online melalui google form adalah:

1. Peserta yang mengisi google form sebanyak 34 orang dengan rata-rata usia:

Tabel 3. Peserta yang mengisi survei

| Usia | Jumlah |
|------|--------|
| 16 | 2,9% |
| 17 | 2,9% |
| 18 | 2,9% |
| 20 | 2,9% |
| 21 | 23,5% |

| | |
|----|-------|
| 22 | 23,5% |
| 23 | 23,5% |
| 24 | 2,9% |
| 25 | 8,8% |
| 26 | 2,9% |
| 27 | 2,9% |

Rata-rata usia 21,22,23 paling banyak mengisi form di bandingkan usia yang lainnya pada tabel 3.

2. Peserta yang berjenis kelamin laki-laki dan perempuan sebesar:

Tabel 4. Jenis Kelamin yang mengisi survei.

| Jenis kelamin | Jumlah |
|---------------|--------|
| Laki-laki | 50% |
| Perempuan | 50% |

Tabel 4 peserta yang mengikuti survey ini berjumlah sama rata antara laki-laki dan perempuan.

3. Tingkat kesadaran dan keamanan informasi.

Tabel 5. Pertanyaan tentang tingkat kesadaran dan keamanan Informasi

| Pertanyaan | Jumlah | | |
|--|--------|------------|--------------|
| | Setuju | Tidak tahu | Tidak setuju |
| Data yang anda input aman dari orang yang tidak berhak mengakses | 79,4% | 17,6% | 3% |
| Sistem mempunyai backup data yang bagus | 82,4% | 14,7% | 2,9% |
| Data anda tidak hilang meskipun listrik mati mendadak | 76,5% | 17,6% | 5,9% |
| Data anda tidak hilang meskipun smartphone anda rusak | 76,5% | 11,8% | 11,8% |
| Sistem informasi jarang crash | 50% | 38,2% | 11,8% |

Hasil rata-rata pada tabel 5 menunjukkan bahwa 72,96% setuju dengan tingkat kesadaran dan keamanan informasi. Dan 19,98% tidak tahu akan tingkat kesadaran dan keamanan informasi, serta 7% memilih tidak setuju dengan kesadaran dan keamanan informasi.

4. Attitude

Tabel 6. Pertanyaan tentang attitude

| Pertanyaan | Jumlah | | |
|------------|--------|------------|--------------|
| | Setuju | Tidak tahu | Tidak setuju |

| | | | |
|--|-------|-------|------|
| Saya sadar bahwa smartphone berbasis android mendapatkan serangan yang dapat memberikan akses kepada penyerang untuk mencuri data informasi pribadi | 70,6% | 26,5% | 8,8% |
| Saya sadar bahwa beberapa smartphone Android tertentu sudah tertanam atau diselipkan backdoor perangkat keras pada firmware sejak dari pabrikannya | 55% | 44,1% | 2,9% |
| Saya sadar bahwa penggunaan aplikasi tidak diunduh dari google play store atau repositori resmi dapat meningkatkan resiko serangan berbasis backdoor | 70,6% | 29,4% | 0% |
| Saya sadar untuk mempertimbangkan hak akses apa saja yang dibutuhkan suatu aplikasi sebelum meng-instalnya (termasuk dari Google Play Store atau repositori resmi lainnya) | 85,3% | 14,7% | 0% |
| Saya sadar bahwa smartphone yang aman digunakan adalah yang telah lulus "Build Test Suite" dan telah mempunyai sertifikasi OEM (Original Equipment Manufacture) atau juga bisa disebut barang original | 82,4% | 14,7% | 2,9% |

Hasil rata-rata pada tabel 6 dari pertanyaan tentang attitude menunjukkan bahwa 72,78% setuju dengan attitude kesadaran dan keamanan informasi. Sedangkan 25,88% dari hasil survei menjawab tidak tahu, serta 3% menjawab tidak setuju dengan attitude kesadaran dan keamanan informasi.

5. Knowledge

Tabel 7. Pertanyaan tentang knowledge

| Pertanyaan | Jumlah | | |
|--|--------|------------|--------------|
| | Setuju | Tidak tahu | Tidak setuju |
| Smartphone berbasis Android berpotensi mendapatkan serangan berbasis backdoor yang dapat memberikan akses kepada penyerang untuk mencuri data informasi pribadi pengguna | 50% | 41,2% | 8,8% |
| Beberapa smartphone Android tertentu sudah tertanam atau diselipkan backdoor perangkat keras pada firmware sejak dari pabrikannya | 45,5% | 54,5% | 0% |
| Penggunaan aplikasi yang tidak diunduh dari Google Play Store atau repositori resmi lainnya dapat meningkatkan risiko serangan berbasis backdoor | 70,6% | 23,5% | 5,9% |

| | | | |
|---|-------|-------|------|
| Sebelum install suatu aplikasi (termasuk dari Google Play Store atau repositoriresmi lainnya), perlu dipertimbangkan hak akses apa saja yang dibutuhkannya untuk berjalan | 85,3% | 11,8% | 2,9% |
| Smartphone yang aman digunakan adalah yang telah lulus "Build Test Suite" dan telah mempunyai sertifikasi OEM atau "Original Equipment Manufacture" atau jugabisa disebut barang original | 81,8% | 18,2% | 0% |

Hasil rata-rata pada tabel 7 dari pertanyaan tentang knowledge menunjukkan hasil 66,64% setuju dengan knowledge, 29,84% menjawab tidak tahu, serta 4% menjawab tidak setuju dengan knowledge

6. Behavior

Tabel 8. Pertanyaan tentang behavior

| Pertanyaan | Jumlah | | |
|--|--------|------------|--------------|
| | Setuju | Tidak tahu | Tidak setuju |
| Saya terbiasa untuk melakukan langkah-langkah pencegahan atas serangan berbasis backdoordi smartphoneAndroid saya | 66,7% | 30,3% | 3% |
| Saya terbiasa untuk tidak menggunakan smartphoneAndroid tertentu yang berpotensi telah tertanam atau diselipkan backdoorperangkat keras pada firmware sejak dari pabrikannya. | 61,8% | 35,3% | 2,9% |
| Saya terbiasa untuk tidak menggunakan aplikasi yang tidak diunduh dari Google Play Store atau repositoriresmi lainnya | 67,6% | 14,7% | 17,6% |
| Saya terbiasa melakukan pertimbangan hak akses apa saja yang dibutuhkan suatu aplikasi sebelum meng-installnya, termasuk dari Google play Store atau repositoriresmi lainnya | 76,5% | 23,5% | 0% |
| Saya terbiasa untuk hanya menggunakan smartphoneAndroid yang telah lulus "Build Test Suite" dan telah mempunyai sertifikasi OEM(Original Equipment Manufacture) atau juga bisa disebut barang original | 81,8% | 18,2% | 0% |

Hasil rata-rata pada tabel 8 menunjukkan 70,88% setuju dengan behavior pada kesadaran dan keamanan informasi. Dan 24,40% tidak tahu dengan behavior, serta 5% tidak setuju dengan behavior pada kesadaran dan keamanan informasi.

Menjaga privasi sangatlah penting bagi pengguna smartphone karena data yang kita unggah ke media sosial bisa berupa data yang berharga ataupun data diri kita. Cara agar data kita tetap aman dari pencurian atau orang yang tidak punya hak akses adalah sebagai berikut:

1. Selalu mengupdate *system* smartphone yang terbaru.
2. Menggunakan *password* atau kata sandi yang rumit dan perbaharui kata sandi 1 bulan sekali.
3. Jangan gunakan atau menginstall aplikasi yang mencurigakan karena bisa saja aplikasi tersebut berupa phishing atau memiliki virus yang bisa mengambil data di smartphone.
4. Mengikuti langkah-langkah untuk melengkapi profil dari aplikasi tempat anda menyimpan data.

5. Kesimpulan

Berdasarkan penelitian tersebut, disimpulkan bahwa tingkat kesadaran keamanan informasi dan privasi pengguna smartphone di Kota Bandung berada pada kriteria yang baik. Hal ini ditunjukkan oleh tingkat kesadaran keamanan informasi sebesar (72,96%). Dan pada hasil attitude mendapatkan hasil (72,78%), pada knowledge mendapatkan hasil rata-rata (66,64%), serta hasil dari behavior mendapatkan hasil rata-rata sebesar (70,88%). Maka hasil dari penelitian tersebut, dapat disimpulkan bahwa pengguna smartphone di kota Bandung memiliki tingkat kesadaran yang baik dalam menjaga keamanan informasi dan privasinya. Oleh karena itu, diharapkan untuk penelitian selanjutnya dapat dilakukan penelitian ini kembali untuk menganalisis faktor-faktor tersebut karena di khawatirkan para pengguna smartphone dimasa selanjutnya mengalami penurunan akan kesadaran keamanan dan privasi tersebut.

6. Daftar Pustaka

- [1] Kruger, H., & W.D, K. (2006). *A prototype for assessing information security Awareness*. Computer & Security
- [2] Mylonas, A. K., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security. Delegate the smartphone user? Security awareness in smartphone platforms. Computers & Security*, 47.
- [3] Ngafifi, M. (2014). *Kemajuan teknologi dan pola hidup manusia dalam perspektif sosial budaya*. Sukoharjo: Jurnal pembangunan pendidikan fondasi dan aplikasi.
- [4] Rizal, A. (2021). *Rata-rata waktu orang indonesia habiskan untuk media sosial*. Jakarta: Info komputer
- [5] Sari, P. K. (2014). Measuring information security awareness of Indonesian smartphone users. *Measuring information security awareness of Indonesian smartphone users*, 9.
- [6] Syafrizal, M. (2007). *Standar Sistem Manajemen Keamanan Informasi* . Yogyakarta: STMIK AMIKOM Yogyakarta .
- [7] Witman, M. E. (2011). *Principles of Information security*. Atlanta: Atlanta Cengage Learning
- [8] Xu, G., & Rosson, c. (2012). *Measuring Mobile Users' Concerns for*. Orlando: Thirty Third International Conference on Information Systems.