Jurnal TEKINKOM, Volume 2, Nomor 2 Desember 2019 *E-ISSN: 2621-3079*
DOI 10.37600/tekinkom.v2i2.113 *ISSN: 2621-1556*

UJI TINGKAT KESADARAN KEAMANAN INFORMASI PENGGUNA SMARTPHONE (STUDI KASUS: AMIK LABUHAN BATU)

Ibnu Rasyid Munthe [1)], Iwan Purnama [2)],
[1] Program Studi Manajemen Informatika, Fakultas Sains dan Teknologi Universitas Labuhanbatu
email: ibnurasyidmunthe@gmail.com
[2] Program Studi Teknologi Informasi, Fakultas Sains dan Teknologi Universitas Labuhanbatu
email: iwanpurnama2014@gmail.com

Abstract

Based on statistical data, it is known that Android is the most popular smartphone with the largest number of users in the world, which is around 1.8 billion users. The high number of users also invites many cases of information security and privacy caused by a lack of awareness from users such as spam, spoofing / phishing, network incidents, malware, uploading something of a personal nature such as photos, telephone numbers, addresses or not having antivirus. This study aims to find out about information security and privacy of Android smartphone users by measuring the problem of the dimension of awareness (attitude, knowledge and behavior) with seven focus areas of information security namely trust in app repositories, misconception about app testing, security and agreement messages, pirated application, adoption of security control, spam sms and report of security incidents and three focus areas on privacy namely perceived surveillance, perceived intrusion, secondary use of information. This research uses analytical hierarchy process (AHP) method to measure the level of information security awareness and privacy of smartphone users. Overall, the results of the study indicate that information security has an average level of awareness (71%). But in the focus area the report for security incidents has a poor level of awareness (37%) this is because users prefer to solve their own information security problems experienced and privacy has an average level of awareness (76%). While the secondary use of information in the attitude dimension has a low level of awareness (66%). Based on these findings, it can be concluded that smartphone users at AMIK Labuhan Batu have a poor level of awareness in maintaining information security and privacy.

Keywords*: Website Service Quality, WebQual, User Satisfaction, Multiple Linear Regression*

1. PENDAHULUAN

Di era teknologi informasi ini smartphone menjadi kebutuhan untuk bisa berkomunikasi dan berbagi informasi seperti mengirim SMS atau email, Kemudian diikuti oleh pesain seperti Apple dengan IOS milikinya yaitu sekitar 463 juta penguna, Windows dengan 45 juta pengguna, disusul Blackberry dengan jumlah pengguna sebanyak 19 juta, serta jenis smartphone lainnya dengan 31 juta pengguna. Di Indonesia sendiri, Menurut website Statista (2016), pangsa pasar yang dimiliki oleh sistem operasi mobile di Indonesia, pada awal bulan Januari 2016, 74,2% dari total pengguna smartphone dimiliki oleh sistem operasi Android berarti sekitar 82.140.000 orang menggunakan smartphone Android dari total pengguna smartphone di Indonesia. Dilansir Gemalto (2015), sektor teknologi menduduki peringkat keempat (12%) yang memiliki jumlah laporan pelanggaran sebanyak 84.394.833 laporan (top 7 sektor dengan jumlah laporan pelanggaran).

Berdasarkan data dari Indonesia Computer Emergency Response Team atau IDCERT (2015), dengan beberapa responden dari penyedia telekomunikasi, dilaporkan bahwa insiden mulai bulan Januari sampai Februari 2015 adalah 30,99% spam; 27.31% respon terhadap laporan yang masuk. 15.67% hak kekayaan intelektual; 4,53% spoofing/phising; 3,98% network incident; dan 3.18% adalah malware. Dilansir Symantec (2015) jumlah jenis malware yang ditemukan dalam sistem operasi

DOI 10.37600/tekinkom.v2i2.113 *ISSN: 2621-1556*

Android terus meningkat tahun dari 2011 yang hanya 71 jenis malware; 174 jenis malware di tahun 2012; 231 jenis malware di tahun 2013; 277 jenis malware di tahun 2014; 295 jenis malware di tahun 2015 dan akan terus bertambah jenis malware yang akan ditemukan sistem operasi Android tiap tahunnya. Dilansir oleh laporan Symantec (2015), 46%, mayoritas pelanggaran yang disebabkan oleh attacker/hacker. Namun, 22% lebih dari pelanggaran diklasifikasikan sebagai "tidak sengaja dibuat publik," dan 21% adalah karena pencurian atau kehilangan komputer atau perangkatnya dan 10% adalah karena adanya keterlibatan orang dalam. Semua jenis pelanggaran data dapat dicegah jika data dienkripsi, secara efektif dapat menghilangkan dampak dari data ini jatuh ke tangan yang salah. salah satu faktor yang menjadi pemicu terjadinya pelanggaran keamanan informasi dan privasi adalah karena pengguna smartphone memiliki kesadaran yang tidak memadai dalam menggunakan smartphone dengan aman, beberapa dari mereka memiliki pengetahuan yang cukup memadai dalam penggunaan smartphone tetapi mereka tidak menerapkannya dengan baik.

Menurut Xu et al, praktik agresif seperti akses data yang digunakan oleh pengembang aplikasi mobile dan sistem operasi telah memperburuk masalah privasi di antara pengguna (smartphone). Kekhawatiran ini terkait dengan 'koleksi otomatis' dari pengguna perangkat mobile, informasi keberadaan secara real-time, dan kerahasiaan data yang dikumpulkan seperti lokasi, identitas pribadi, dan perilaku sehari-hari. Berbeda dengan internet konvensional, platform mobile memungkinkan untuk real-time dan komunikasi data dan transmisi yang selalu menyala, yang menimbulkan ancaman privasi.[1]

Informasi Privasi menjadi kekhawatiran pengguna tentang kemungkinan kehilangan privasi sebagai akibat dari pengungkapan informasi kepada pihak ketiga seperti pengembang aplikasi. Teori ini memaparkan bahwa smartphone yang sangat dikenal khususnya Android merupakan sistem operasi mobile phone yang memiliki resiko yang besar, masih banyak pengguna smartphone yang belum menyadari aturan keamanan dan privasi yang harus diperhatikan dalam menggunakan smartphone.

2. METODE PENELITIAN

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. Menurut McLeod dan Schell keamanan informasi ditujukan untuk mencapai tiga tujuan utama, yaitu kerahasiaan ketersediaan, dan integritas[2]. Dalam penelitian ini, keamanan informasi dibagi menajadi 7 indikator 5 diantaranya trust in application repository, misconception about app testing, security and agreement message, pirated applicaion, dan adoption of security control ditambah 2 indikator seperti spam sms dan report of security incidents [3].

Terdapat empat definisi privasi informasi yaitu privasi sebagai hak asasi manusia, privasi sebagai komoditas, privasi sebagai keadaan akses terbatas, dan privasi sebagai kemampuan untuk mengendalikan informasi tentang diri sendiri. 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 [3]. 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 (2006), 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)[4].

Jenis penelitian yang digunakan adalah penelitian kuantitatif dimana data dikumpulkan dengan menggunakan kuesioner. Penelitian ini memiliki 42 pertanyaan dari kesadaran keamanan informasi dan 27 pertanyaan dari kesadaran privasi untuk menguji attitude, knowledge dan behavior dalam perspektif penggunaan smartphone Android. Beberapa pertanyaan dijawab dalam skala 3 poin yaitu setuju, tidak tahu dan tidak setuju (dimensi attitude dan knowledge), sementara yang lain hanya membutuhkan jawaban yang setuju atau tidak setuju (dimensi behavior). Contoh pertanyaan yang diajukan dapat dilihat di Tabel 1. Kuesioner disebar secara online.

Tabel 1. Contoh Pertanyaan

Dimensi	Pertanyaan	Jawaban
Attitude	Saya mempertimbangkan keamanan sebelum menginstal Aplikasi dari repositori aplikasi	1. Setuju 2. Tidak Tahu 3. Tidak
Knowledge	Jika saya tidak mempertimbangkan keamanan sebelum menginstall aplikasi dari repository aplikasi, saya bisa mengalami gangguan keamanan informasi	1. Setuju 2. Tidak Tahu 3. Tidak
Behavior	Saya selalu mempertimbankan sebelum menginstal aplikasi dari repository aplikasi	1. Setuju 2. Tidak

tiga fokus area privasi yaitu perceived surveillance, perceived intrusion dan secondary use information. Untuk menguji validitas setiap item dalam kuesioner, penulis menggunakan korelasi Pearson Product Moment dimana setiap item yang memiliki koefisien korelasi sama atau lebih dari 0,3 adalah valid. Untuk pengujian reliabilitas penulis menggunakan metode Alpha Cronbach, dimana koefisiennya harus sama atau lebih dari 0,5. pembobotan ditentukan dengan menggunakan analytical hierarchy process (AHP). Pendekatan AHP menggunakan perbandingan berpasangan untuk memberikan evaluasi subyektif terhadap faktor berdasarkan pertimbangan dan pendapat profesional manajemen. Setiap dimensi memiliki bobot yang akan digunakan dalam pehitungan skor kesadaran. Bobot tersebut didefinisikan pada Tabel 2. Pembobotan Dimensi sebagai berikut.

Tabel 2. Pembobotan Dimensi

Dimensi	Bobot
Attitude	20
Knowledge	30
Behavior	50

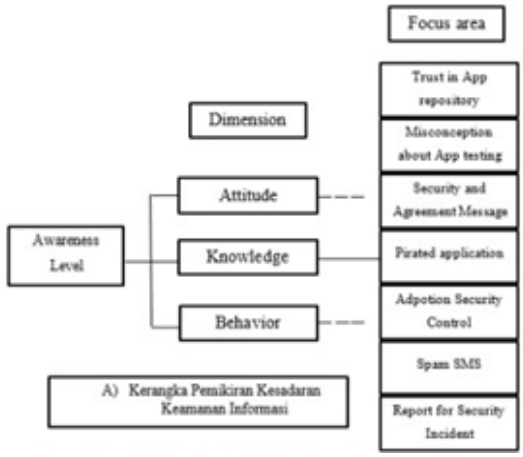
Kerangka pemikiran dari penilitian ini menggunakan model yang mengadaptasi teori psikologi sosial yang mengusulkan tiga komponen untuk mengukur cara yang menguntungkan atau tidak menguntungkan terhadap objek tertentu. Komponen tersebut digunakan untuk mengembangkan tiga dimensi yang dikenal sebagai knowledge (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[5].

Kerangka pemikiran kesadaran keamanan informasi pada Gambar 1 dengan menggunakan model Krueger dan Kerney (2006) untuk mengukur tingkat kesadaran dari tiap-tiap fokus area yang lima diantaranya diadaptasi dari Mylonas et al. (2013) yaitu trust in app repository, misconception about app testing, security and agreement message, prirated 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. Lalu misconception about app testing yang bisa dilihat dari kesadaran pengguna untuk menguji aplikasi pada repositorty aplikasi. Security and agreement message yang diketahui dari kesadaran pengguna tentang persetujuan keamanan

DOI 10.37600/tekinkom.v2i2.113 *ISSN: 2621-1556*

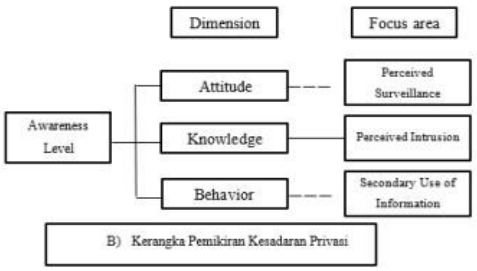
aplikasi, persetujuan lisensi, dan konsekuensi penggunaan aplikasi. Selanjutnya prirated application berupa kekhawatiran pengguna untuk menginstal aplikasi bajakan dan banyaknya aplikasi bajakan yang mengandung malware. Kemudian adoption security control yang terlihat dari kontrol keamanan yang digunakan pengguna, anti virus smartphone pengguna, adanya kehadiran virus, dan lain sebagainya[6].

Berikut ini adalah metode yang diadopsi dari model Kruger dan Kearney seperti yang ditunjukan pada Gambar 1. Kerangka Pemikiran Kesadaran Keamanan Informasi.



Gambar 1. Kerangka Pemikiran Kesadaran Keamanan Informasi

Adapun dua fokus area lainya dari kerangka pemikiran kesadaran keamanan informasi pada Gambar 3 yaitu spam sms dan report for security incident. Ketujuh fokus area yang telah disebutkan di atas, digabungkan bertujuan agar penelitian lebih konprehensif untuk mengukur kesadaran kaamanan informasi. Sedangkan kerangka pemikiran kesadaran privasi dapat dilihat pada Gambar 2.



Gambar 2. Kerangka pemikiran kesadaran privasi.

Pada Gambar 2, Kerangka pemikiran kesadaran privasi juga yang menggunakan perceived surveillance, perceived intrusion, dan secondary use of information untuk mengukur kesadaran privasi pengguna smartphone. Fokus area perceived surveillance adalah untuk mengetahui apakah perangkat lokasi yang ada di smartphone memantau kegiatan pengguna, aplikasi mobile yang dapat mengumpulkan banyak informasi pengguna menimbulkan kekhawatiran pengguna, dan aplikasi mobile pada perangkat mobile yang dapat memantau kegiatan pengguna menimbulkan kekhawatiran pengguna[7].

Sedangkan fokus area perceived intrusion adalah untuk mengetahui apakah penggunaan aplikasi mobile menimbulkan rasa tidak nyaman bagi penggunaya, informasi pribadi pengguna yang lebih mudah tersedia untuk orang lain, dan akibat dari penggunaan aplikasi mobile[8]. Kemudiaan untuk fokus area secondary use of information adalah untuk mengetahui apakah Aplikasi mobile dapat menggunakan informasi pribadi pengguna untuk tujuan lain tanpa izin otoritas dari pengguna, aplikasi dapat menggunakan informasi pribadi pengguna untuk tujuan lain, dan aplikasi mobile dapat berbagi informasi pribadi pengguna dengan entitas lain tanpa otorisasi pengguna. 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.

3. HASIL DAN PEMBAHASAN

Penelitian ini mengambil sampel sebanyak 100 responden dari mahasiswa AMIK Labuhan Batu dimana kuesioner didistribusikan oleh peneliti pada bulan Maret 2019 di AMIK Labuhan Batu. Di bawah ini merupakan karakteristik dari responden yang menggunakan smartphone Android[9] Tabel 3. Jenis Kelamin Responden.

DOI 10.37600/tekinkom.v2i2.113 *ISSN: 2621-1556*

Tabel 3. Jenis kelamin responden

No	Jenis Kelamin	Persentase
1	Laki-laki	52%
2	Perempuan	48%

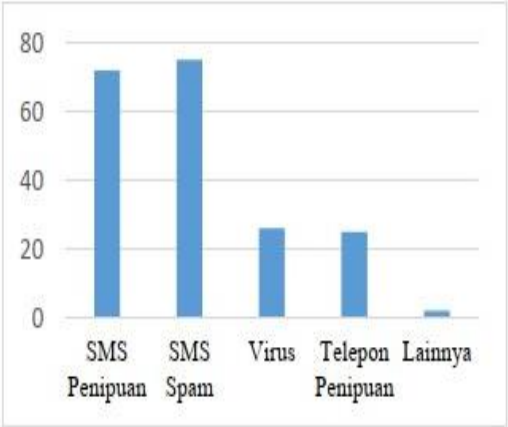
Pada Tabel 3 menggambarkan responden bedasarkan jenis kelamin dimana jumlah responden laki- laki lebih banyak dari responden perempuan. Hal ini memperlihatkan bahwa mayoritas responden pada penelitian adalah laki-laki. Kemudian untuk karakteristik responden dilihat dari segi usia dapat dilihat pada Tabel 4 Usia Responden.

Tabel 4. Usia responden

No	Usia	Persentase
1	< 16 Tahun	2%
2	16-18 Tahun	8%
3	18-23 Tahun	81%
4	23-30 Tahun	8%
5	30-40 Tahun	1%

Pada Tabel 4 Usia Responden diatas menunjukan jumlah responden penelitian ini didominasi oleh kategori usia 18-23 tahun. Selain itu, data ini juga memperlihatkan bahwa pengguna smartphone Android kebanyakan berasal dari kalangan anak muda. Dari banyaknya pengguna smartphone yang menjadi responden pada penelitian ini, diketahui juga bahwa pengguna tersebut pernah mengalami gangguan informasi pada saat menggunakan smartphone. Detail data dapat dilihat pada Tabel 5. Pengalaman Gangguan Keamanan Informasi.

Berdasarkan hasil survei, responden yang pernah mengalami gangguan keamanan informasi ada sebanyak 91% sedangkan 9% sisanya belum pernah mengalami gangguan keamanan informasi. Sehingga dapat diketahui bahwa harpir semua pengguna smartphone Android pernah mengalami gangguan keamanan informasi. Gangguan keamanan informasi ini bisa berasal beberapa faktor seperti sms penipuan, sms spam, virus, telepon penipuan, dan lain-lain. Data pengalaman gangguan keamanan informasi pengguna smartphone berdasarkan jenis ancaman gangguannya dapat dilihat pada Gambar 3.



Gambar 3. Ancaman Gangguan Keamanan Informasi.

Responden banyak mengalami gangguan keamanan informasi berupa sms spam dengan jumlah 75 responden, lalu pada gangguan keamanan informasi berupa sms penipuan sebanyak 72 responden, lalu responden yang gangguan keamanan informasi berupa virus sebanyak 26 responden, dan sebanyak 25 responden telah mengalami gangguan berupa telepon penipuan. Berdasarkan data yang ditampilkan pada Gambar 6, dapat diketahui bahwa pengguna smarphone Android merasa terganggu oleh sms spam yang bermunculan pada ponselnya dan

Tabel 5. Pengalaman Ganguan Keamanan informasi

No	Pengalaman Gangguan	Persentase
1	Ya	91%
2	Tidak	9%

mengalami gangguan privasi dapat dilihat pada Tabel 6 Pengalaman Gangguan Privasi.

Tabel 6. Pengalaman Ganguan Privasi

No	Pengalaman Gangguan	Persentase
1	Ya	67%
2	Tidak	33%

Pada Tabel 7 menunjukan persentase jumlah responden yang pernah mengalami gangguan

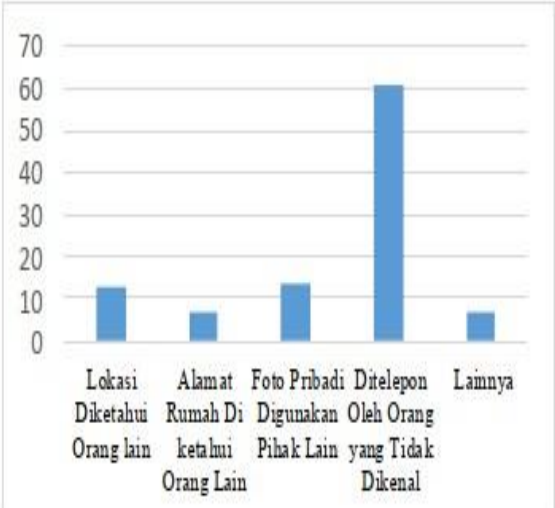
DOI 10.37600/tekinkom.v2i2.113 *ISSN: 2621-1556*

privasi yaitu ada sebanyak 67%. Sedangkan 33% sisanya belum pernah mengalami gangguan privasi.

Tabel 7. Kriteria Kesadaran

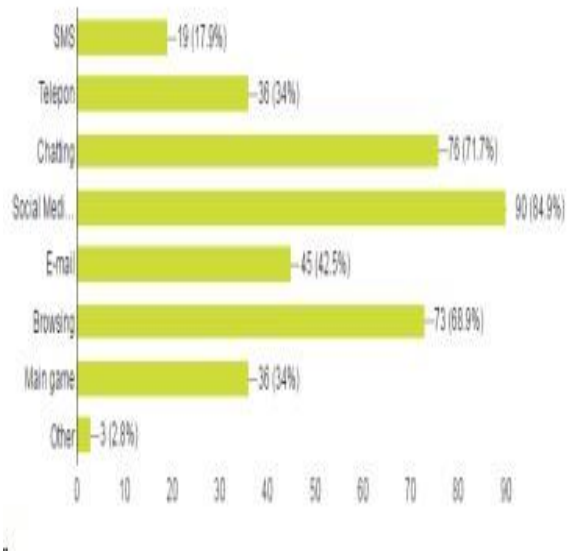
Kriteria	Nilai (%)	Tindakan
Baik	77, 78- 100	Tidak dibutuhkan tindakan
Rata-rata	55,56-77,77	Berpotensi tindakan diperlukan
Buruk	33,33-55,55	Tindakan diperlukan

Sehingga dapat diketahui bahwa harpir semua pengguna smartphone Android pernah mengalami gangguan privasi. Gangguan keamanan informasi ini bisa disebabkan oleh beberapa hal seperti lokasi pengguna yang diketahui oleh orang lain, alamat rumah yang diketahui oleh orang lain, foto pribadi yang digunakan orang lain tanpa izin, adanya telepon dari orang yang tidak dikenal, dan lain-lain. Data hasil survei berdasarkan gangguan keamanan informasi pengguna smartphone berdasarkan jenis gangguan privasi yang dialami responden dapat dilihat pada Gambar 4.



Gambar 4. Ancaman Gangguan Privasi

Banyaknya jumlah responden yang mengalami gangguan privasi berupa telepon dari orang yang tidak dikenal ada sebanya 61 responden. Lalu banyaknya responden yang mengalami gangguan privasi berupa foto pribadi digunakan oleh pihak lain ada sebanyak 14 responden. Kemudian jumlah responden yang mengalami gangguan privasi berupa lokasi diketahui oleh orang lain ada sebanyak 13 responden, dan sebanyak 7 responden telah mengalami gangguan privasi berupa alamat rumah diketahui orang lain. Berdasarkan data yang ditampilkan pada Gambar 5, dapat diketahui bahwa pengguna smarphone Android merasa terganggu oleh telepon dari orang yang tidak dikenal muncul di ponselnya dan mayoritas responden mengalami gangguan tersebut.



Gambar 5. Ancaman Gangguan Privasi

Berdasarkan hasil survei yang diperlihatkan bahwa pengguna menggunakan smartphone untuk social media (84,9%), chatting (71,7%), browsing (69,8%), email (42,5%), main game dan telepon (34%), SMS (17,9%), lainnya (2,8%). Hal tersebut menunjukkan bahwa pengguna smartphone yang menggunakan internet semakin meningkat dan untuk telpon dan SMS menurun.

Skor hasil masing- masing fokus area dan dimensi kemudian dikelompokkan sebagai kriteria kesadaran yang sesuai dengan Tabel.3. Nilai interval dari kriteria tersebut didasarkan pada nilai garis kontinum dimana nilai maksimumnya adalah 100% dan skor minimumnya adalah 33,33%. Setiap kriteria juga mengidentifikasikan apakah suatu focus area memerlukan tindakan untuk perbaikan atau tidak. Tabel 8. Tingkat Kesadaran Keamanan Informasi

Tabel 8. Tingkat Kesadaran Keamanan Informasi

Fokus Area	Dimensi (Bobot)			
	A	K	B	Total
	20	30	50	100
User's trust in app repository	50	58	82	**68**
Misconception about application testing	85	59	78	**74**
Security Agreement Messages	58	81	87	**80**
Pirated Application	81	88	83	**84**
Adoption of Security Control	67	67	50	**58**
Spam SMS	73	70	94	**83**
Report for Security Incidents	61	56	37	**50**
Total Awareness/ Dimensi	**69**	**68**	**73**	**71**

Keterangan
A = Attitude; K = Knowledge; B = Behavior;

Dari tingkat kesadaran keamanan informasi yang didapat seperti pada Tabel 8, dengan hasil sebagai berikut:

1. Total keseluruhan tingkat kesadaran keamanan informasi adalah 71%. Hal ini mengindikasikan bahwa tingkat kesadaran keamanan informasi di tingkat rata-rata atau berada ditingkat memuaskan. Tingkat kesadaran tertinggi terdapat pada dimensi behavior yaitu 73%, lalu dimensi attitude dengan 69% dan dimensi knowledge memiliki tingkat kesadaran terkecil yaitu 68%. Hal ini menunjukkan bahwa attitude, knowledge, dan behavior memiliki kriteria rata-rata.
2. Pada fokus area security agreement messages, pirated application, dan spam SMS memiliki kritetria kesadaran yang baik dan tidak memerlukan tindakan untuk perbaikan. Dari hasil yang didapatkan dari tingkat kesadaran keamanan informasi menunjukkan bahwa fokus area yang memerlukan tindakan maupun yang masih berpotensi (tingkat rata-rata dan buruk) sebagai berikut :

a. User's trust in app repository

Pada dimensi attitude memiliki kriteria kesadaran buruk (50%). Berdasarkan pertanyaaan yang diberikan, sebagian pengguna tidak menganggap mengunduh aplikasi di play store aman dipasang pada smartphone pengguna. Hal ini dikarenakan setiap aplikasi memiliki hak akses pada smartphone pengguna dan aplikasi dapat mengambil data mereka kapanpun. Kekhawatiran ini membuat responden menganggapnya tidak aman. Hal ini perlu dilakukan tindakan untuk perbaikan. Pada dimensi knowledge memiliki kriteria kesadaran rata-rata (58%) akan tetapi tingkat kesadarannya hampir berada di kriteria buruk. Berdasarakan pertanyaan yang telah diberikan beberapa responden tidak mengetahui jika mengunduh melalui app repository (play store) lebih aman daripada mengunduh ditempat lain. Walaupun begitu responden tetap mengunduh melalui app repository terlihat pada dimensi behavior yang memiliki kriteria bagus.

b. Misconception about application testing

Pada dimensi knowledge memiliki kriteria kesadaran rata-rata (59%) hal tersebut menunjukkan dimensi tersebut harus mendapatkan perhatian. Berdasarkan pertanyaan yang telah diberikan, sebagian pengguna tidak mengetahui apakah aplikasi yang telah di instal pada smartphone mereka telah diuji dulu keamanannya atau belum. Hal ini menunjukkan bahwa pengguna percaya menginstal aplikasi melalui app repository (Play Store).

c. Security agreement messages

Pada dimensi attitude memiliki kriteria kesadaran rata-rata (58%) dengan kriteria kesadaran tersebut menujukkan bahwa dimensi attitude harus mendapatkan perhatian karena mendekati kriteria kesadaran yang buruk. Berdasarkan pertanyaan yang telah diberikan, sebagian pengguna mungkin jarang membaca informasi tentang kebijakan keamanan yang muncul sebelum menginstal aplikasi. Ini mungkin dikarenakan memakan waktu terlalu jika pengguna membaca semua item dalam kebijakan keamanan saat mereka menginstal aplikasi baru. Namun pada dimensi behavior memiliki kriteria kesaradaran yang baik dimana pengguna mematuhi informasi tentang kebijakan keamanan. Hal ini mungkin karena pengguna sudah memahami kebijakan keamanan yang umum.

d. Adoption security control

Pada dimensi attitude dan knowledge memiliki kriteria kesadaran yang sama yaitu memuaskan (67%) hal ini menunjukkan kedua dimensi tersebut harus mendapatkan perhatian

karena berpotensi diperlukannya tindakan. Sedangkan pada dimensi behavior memiliki kriteria kesadaran yang buruk (50%). Berdasarkan pertanyaan yang telah diberikan, pengguna sebagian besar tidak memasang antivirus, password maupun mekanisme keamanan informasi lainnya untuk melindungi smartphone mereka dan pengguna yang memiliki aplikasi antivirus tidak mengupdate secara rutin. Selain itu, rendahnya tingkat behavior mungkin disebabkan karena kurangnya pengetahuan tentang antivirus itu sendiri

e. Spam SMS

Pada dimensi attitude dan knowledge memiliki kriteria kesadaran rata-rata (73% dan 70%). Berdasarkan pertanyaan yang telah diberikan, beberapa pengguna tidak mengetahui bahwa SMS premium dapat mengurangi sejumlah pulsa yang dimiliki pengguna dan beberapa pengguna masih memilih menanggapi SMS dari pihak yang tidak dikenal. Walaupun penyebab rendahnya tingkat kesadaran dimensi attitude dan behavior adalah kurangnya pengetahuan tentang SMS premium, pengguna tidak berlangganan SMS premium dapat dilihat dari tingkat kesadaran pada dimensi behavior sebesar 94% dan memiliki kriteria kesadaran yang baik.

f. Report for security incidents

Pada dimensi attitude dan knowledge memiliki kriteria kesadaran rata-rata (61% dan 56%). Hal tersebut menujukkan bahwa kedua dimensi tersebut harus mendapatkan perhatian dan berpotensi diperlukannya tindakan untuk perbaikan, sedangkan pada dimensi behavior memiliki kriteria yang buruk (37%). Hal tersebut menunjukkan diperlukannya tindakan untuk perbaikan karena rendahnya tingkat kesadaran. Berdasarkan pertanyaan yang telah diberikan dalam hal melaporkan insiden keamanan sebagaian besar pengguna mungkin lebih memilih untuk menyelesaikan sendiri insiden keamanan informasi yang dialami daripada melaporkan kepada pihak developer aplikasi melalui feedback karena telah mengalami gangguan keamanan informasi.

Tabel 9. Tingkat Kesadaran Privasi

Fokus Area	Dimensi (bobot)			
	A	K	B	Total
	20	30	50	100
Perceived Surveillance	75	78	80	**78**
Perceived Intrusion	68	72	71	**71**
Secondary Use of Information	78	66	83	**77**
Total Awareness/ Dimension	**74**	**72**	**78**	**76**

Keterangan
A = Attitude; K = Knowledge; B = Behavior;

Dari tingkat kesadaran privasi pada Tabel 9. Kesadaran Privasi didapatkan hasil sebagai berikut :

1. Total keseluruhan tingkat kesadaran privasi adalah 76%. Hal ini mengindikasikan bahwa tingkat kesadaran keamanan informasi di tingkat ditingkat memuaskan.
2. Tingkat kesadaran tertinggi terdapat pada dimensi behavior yaitu 78%, lalu dimensi attitude dengan 74% dan dimensi knowledge memiliki tingkat kesadaran terkecil yaitu 72%. Hal ini menunjukkan bahwa attitude, knowledge memiliki kriteria rata-rata atau memuaskan, sedangkan dimensi behavior memiliki kriteria kesadaran yang baik.
3. Pada fokus area perceived surveillance memiliki kritetria kesadaran yang baik dan tidak memerlukan tindakan untuk perbaikan.
4. Tidak ada satupun fokus area dan dimensi dari tingkat kesadaran privasi yang kriteria kesadaran yang buruk (tingkat kesadaran dibawah 55,56%).

Dari hasil yang didapatkan dari tingkat kesadaran privasi menunjukkan fokus area yang memerlukan tindakan maupun yang masih berpotensi (tingkat rata-rata dan buruk) sebagai berikut

1. Perceived surveillance

Pada dimensi attitude memiliki kriteria kesadaran yang memuaskan (75%). selain itu, pada dimensi knowledge dan behavior sudah memiliki kriteria yang baik dan tidak diperlukan tindakan untuk perbaikan. Berdasarkan pertanyaan yang telah diberikan sebagian besar pengguna sudah mengetahui bahwa aplikasi dapat mengumpulkan informasi pengguna smartphone dari hak akses yang diberikan oleh aplikasi terutama pada fitur global positioning system (GPS) yang dapat

DOI 10.37600/tekinkom.v2i2.113 *ISSN: 2621-1556*

mengetahui lokasi pengguna ketika menyalakan fitur tersebut. Selain itu, pengguna juga sudah paham untuk selalu mematikan fitur GPS ketika sudah tidak diperlukan lagi.

2. Perceived intrusion

Pada dimensi attitude, knowledge, dan behavior memiliki kriteria kesadaran rata-rata, dimana tingkat kesadaran attitude sebesar 68% knowledge sebesar 72% dan behavior sebesar 71%. Hal tersebut menunjukkan bahwa dimensi attitude, knowledge, behavior berpotensi perlu dilakukan tindakan untuk perbaikan. Berdasarkan pertanyaan yang telah diberikan sebagian besar pengguna sudah menyadari bahwa informasi pribadi pengguna lebih tersedia untuk orang lain seperti foto, alamat dan nomor telepon pengguna. Contohnya aplikasi path orang lain dapat menyimpan foto yang telah diunggah oleh pengguna. Selain itu sebagian besar pengguna sudah menyadari bahwa situs dapat mengetahui minat pengguna berdasarkan history dan cookies penulusaran dan selalu rutin menghapus agar situs tidak mengoleksi data pengguna.

3. Secondary use of information

Pada dimensi attitude dan behavior sudah memiliki kriteria kesadaran yang baik sedangkan, pada dimensi knowledge memiliki kriteria kesadaran rata-rata (66%). Hal tersebut menunjukkan bahwa dimensi knowledge berpotensi perlu dilakukan tindakan untuk perbaikan. Berdasarkan pertanyaan yang telah diberikan sebagian pengguna kurang pengetahuan bahwa aplikasi bisa saja menggunakan informasi pribadi pengguna tanpa izin terlebih dahulu pengguna juga kurang menyadari bahwa aplikasi bisa memberikan informasi pribadi pengguna kepada entitas lain atau untuk tujuan lain. Walaupun kurangnya pengetahuan akan aplikasi yang dapat bersifat intrusi pengguna hanya memberikan informasi mana yang akan diberikan pada aplikasi terlihat pada dimensi behavior yang memiliki kriteria kesadaran yang baik.

4. KESIMPULAN

Berdasarkan penelitian kami, dinyatakan bahwa tingkat kesadaran keamanan informasi dan privasi pengguna smartphone di AMIK Labuhan Batu ada berada pada kriteria rata-rata. Hal ini ditunjukkan oleh tingkat kesadaran keamanan informasi sebesar 71% dan privasi 76%. Namun terdapat beberapa fokus area yang harus diperbaiki agar bisa mengalami peningkatan potensial terutama pada report for security incidents (37%) yang memiliki kriteria kesadaran yang buruk Dengan menerapkan program kesadaran keamanan informasi bagi pengguna smartphone, penulis berharap pengguna smartphone dapat mengerti tentang keamanan dan pengamanan informasi mereka dalam penggunaan smartphone yang biasanya mereka gunakan untuk email, layanan di media sosial, sms, chatting, dan lain-lain. Program kesadaran keamanan ini penting karena Jumlah pengguna smartphone selalu meningkat setiap tahunnya dan mereka menggunakannya untuk berbagai keperluan.

Tingkat kesadaran privasi memiliki kriteria kesadaran rata-rata (76%). Hal ini menunjukkan bahwa secara umum bagus. Namun terdapat beberapa fokus area berpotensi diperlukan tindakan perbaikan yaitu; secondary use of information (66%) pada dimensi knowledge. Pengguna smartphone kurang mengetahui bahwa aplikasi bisa saja menggunakan informasi pribadi pengguna tanpa izin terlebih dahulu, pengguna juga kurang menyadari bahwa aplikasi bisa memberikan informasi pribadi pengguna kepada entitas lain atau untuk tujuan lain.

Terdapat ketimpangan yaitu dimana responden yang mengalami gangguan keamanan informasi (sebesar 91%) hal ini kemungkinan bisa terjadi karena pada fokus area report for security incidents memiliki kriteria kesadaran yang buruk. Oleh karena itu, diharapkan untuk penelitian selanjutnya dapat dikembangkan untuk menganalisis faktor-faktor tersebut seperti mengapa pelanggaran keamanan informasi terhadap pengguna smartphone masih tergolong tinggi.

UCAPAN TERIMAKASIH

Peneliti mengucapkan Terimakasih kepada Direktorat Riset dan Pengabdian Masyarakat, dan Pendidikan Tinggi atas dukungan yang diberikan berupa bantuan dana penelitian yang menunjang berlangsungnya penelitian ini

dengan baik. Melalui SKIM Penelitian Dosen Pemula Tahun Anggaran 2018 Pelaksanaan Tahun 2019

5. REFERENSI

[1] H. Xu, M. B. Rosson, S. Gupta, and J. M. Carroll, "MEASURING MOBILE USERS' CONCERNS FOR INFORMATION PRIVACY," in *Thirty Third International Conference on Information Systems*, 2012, no. Ftc 2009, pp. 1–8.

[2] R. M. Jr, G. S.-J. S. Empat, and U. 2008, *Sistem Informasi Manajemen Edisi 10*. .

[3] P. Kencana Sari, "Measuring Information Security Awareness of Indonesian Smartphone Users," *TELKOMNIKA*, vol. 12, no. 2, pp. 1693–6930, 2014.

[4] H.A.Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Elsevier*, 2006.

[5] I. H. Hann, K. L. Hui, S. Y. T. Lee, and I. P. L. Png, "Overcoming online information privacy concerns: An information-processing theory approach," in *Journal of Management Information Systems*, 2007, vol. 24, no. 2, pp. 13–42.

[6] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the Smartphone User? Security Awareness in Smartphone Platforms †."

[7] y al Sheri and N. . Clarke, "Advances in Communications, Computing, Networks and Security: Proceedings of ... - Paul Dowland, Steven Furnell, University of Plymouth. School of Computing, Communications and Electronics - Google Buku." [Online]. Available:.

[8] J. Yim, J. Ju, H. Jung, and J. Kim, "Image classification using convolutional neural networks with multi-stage feature," in *Advances in Intelligent Systems and Computing*, 2015, vol. 345, pp. 587–594.

[9] N. Martono, *METODE PENELITIAN KUANTITATIF: Analisis Isi dan Analisis Data Sekunder*. RajaGrafindo.