MENGUKUR TINGKAT KESADARAN KEAMANAN INFORMASI PENGGUNA HANDPHONE ANDROID MAHASISWA UNIVERSITAS MALIKUSSALEH DENGAN METODE ANALYTICAL HIERARCHY PROCESS (AHP)

Munirul Ula*, Rizal Tjut Adek, dan Bustami

Program Studi Teknik Informatika, Universitas Malikussaleh, Aceh, Indonesia
**Email: munirulula@unimal.ac.id*

Abstrak

Perkembangan teknologi komunikasi yang begitu cepat, ternyata dikuti oleh bahaya yang besar. Dalam lima tahun terakhir sangat banyak kasus keamanan informasi yang terjadi di Indonesia. Kasus-kasus yang banyak terjadi melalui internet, media social dan juga melalui SMS. Handphone android adalah memiliki konsumen terbesar dikalangan mahasiswa Universitas Malikussaleh, survei pada tahun 2020, 80 persen mahasiswa menggunakan Android. Penelitian ini mengunakan konsumen sebagai variabel untuk mengukur tingkat kesadaran keamanan informasi banyak ancaman melalui mereka. Kesadaran keamanan informasi akan diukur dari pengetahuan, perilaku, dan sikap pengguna terhadap lima area fokus keamanan informasi di bidang telekomunikasi. Bagi pengguna Handphone Android, ancaman keamanan informasi tidak hanya dari Internet, tetapi juga dari panggilan telepon atau SMS. Oleh karena itu, area fokus dalam penelitian ini terdiri dari mematuhi kebijakan keamanan, melindungi data pribadi, penipuan/SPAM SMS, aplikasi seluler, dan melaporkan insiden keamanan. Penelitian ini menggunakan metode analytic hierarchy process (AHP) untuk mengukur tingkat kesadaran keamanan informasi mahasiswa Universitas Malikussaleh yang menggunakan Handphone Android. Secara total, hasilnya menunjukkan bahwa tingkat kesadaran baik (80%). Meskipun pengetahuan dan dimensi sikap adalah kriteria yang baik dari tingkat kesadaran, dimensi perilaku rata-rata. Ini bisa menjadi alasan mengapa masih ada banyak pelanggaran keamanan informasi terhadap pengguna Handphone Android meskipun tingkat kesadaran yang baik.

Kata kunci: *Keamanan informasi, Kesadaran, Pengukuran, Handphone Android, Pengguna.*

Pendahuluan

Ada tiga hal mendasar yang harus dipertimbangkan ketika menerapkan manajemen keamanan informasi dalam suatu organisasi: (1) kerahasiaan informasi sensitif dengan melindunginya dari pengungkapan yang tidak sah atau penyadapan yang cerdas, (2) integritas, dengan menjaga keakuratan dan kelengkapan informasi, (3) ketersediaan, dengan memastikan bahwa informasi dan layanan vital tersedia untuk pengguna yang berwenang ketika diperlukan [1]. Ini dapat menyebabkan pencapaian niat keamanan informasi, yaitu memastikan kelangsungan bisnis dan untuk meminimalkan kerusakan bisnis dengan mencegah dan meminimalkan dampak insiden keamanan [2].

Setiap ancaman potensial dalam organisasi adalah subjek yang memengaruhi manajemen keamanan informasi. Ancaman tersebut dapat dideteksi dengan mengidentifikasi keadaan atau aktivitas yang dapat menyebabkan kerugian atau bahaya bagi organisasi, seperti kehilangan keuangan, tidak adanya data atau sumber daya, atau bahkan hilangnya kredibilitas perusahaan [1]. Banyak produk telah dikembangkan untuk menjamin keamanan informasi. Karena keterbukaan jaringan, kerentanan sistem operasi, risiko keamanan dalam perangkat keras dan perangkat lunak, dan virus jaringan dan serangan jaringan terus bervariasidan setiap hari ancaman ini semakin sulit dihilangkan; sehingga tidak ada kesempatan untuk membangun sistem jaringan keamanan absolut [3]. Hal terpenting dalam manajemen keamanan informasi adalah program kesadaran itu sendiri. Program ini untuk memastikan bahwa semua karyawan mematuhi kebijakan dan prosedur keamanan informasi yang ditetapkan oleh organisasi. Kruger dan Kearney mengatakan bahwa "Tujuan awal atau tujuan kesadaran keamanan informasi adalah untuk memastikan bahwa pengguna komputer menyadari risiko yang terkait dengan penggunaan teknologi informasi serta memahami dan mematuhi kebijakan dan prosedur yang berlaku" [4].

Dilansir Symantec, sektor telekomunikasi berada di peringkat kedua (10%) setelah ritel (27%) yang memiliki risiko dalam pelanggaran data yang dapat menyebabkan pencurian identitas (10 sektor teratas berdasarkan jumlah identitas yang terpapar) [5] di mana Indonesia berada di peringkat kedelapan negara dengan biaya per kapita tertinggi dari pelanggaran data. Tim Tanggap Darurat Komputer Indonesia (ID-CERT) yang disurvei, dengan beberapa responden dari penyedia telekomunikasi, bahwa 53,1% insiden yang dilaporkan dari Maret hingga April 2022 adalah tentang insiden jaringan; 15,4% adalah hak kekayaan intelektual; 12.1% adalah insiden malware; dan 11,4% adalah spam [6]. Pada 2012, jumlah insiden jaringan telah mencapai 76,53%. Oleh karena itu, semua tindakan pencegahan untuk mengurangi insiden ini harus ditingkatkan dan diperkuat oleh penyedia layanan internet, termasuk industri telekomunikasi [7].

Profil Internet Indonesia pada Desember 2020 yang dirilis oleh APJII menginformasikan bahwa 75,7% pengguna internet di Indonesia memanfaatkan Handphone Android sebagai perangkatnya. Pengguna handphone android di Indonesia diprediksi mencapai 71,6 juta orang pada 2015, melonjak dari 23,8 juta pada 2012. Fenomena ini kemungkinan karena harga gadget dan layanan yang murah yang disediakan oleh penyedia telekomunikasi. Namun di sisi lain, penggunaan teknologi mobile juga meningkatkan ancaman keamanan informasi. Selain itu, dengan perkembangan internet dan komputasi cloud yang lebih cepat, masalah keamanan telah menjadi masalah yang luar biasa bagi penyedia layanan cloud. Untuk memanfaatkan manfaat cloud secara penuh, masalah ini perlu ditangani terlebih dahulu [8]. Pada tahun 2010, Yayasan Layanan Konsumen Indonesia (YLKI) mencatat bahwa 17,1% dari 590 keluhan konsumen adalah tentang layanan telekomunikasi, di mana peringkat pertama pada periode tersebut. Sekitar 46,7% dari keluhan tersebut adalah tentang mencuri saldo pelanggan. Pada akhirnya, ini tidak hanya akan mematahkan kepercayaan pelanggan, tetapi juga kredibilitas telekomunikasi, yang merupakan salah satu perhatian dalam manajemen keamanan informasi.

Pengguna sering memiliki kesadaran yang tidak memadai tentang cara menggunakan gadget dengan aman, atau tidak memiliki pengetahuan yang cukup tetapi tidak menerapkannya dengan benar [9]. Pengguna seluler sering menyimpan informasi pribadi dan keuangan di ponsel mereka. Itu membuat mereka menjadi target yang rentan terhadap malware dan phishing. Di era handphone android ini, ada ancaman baru yang berkembang seperti serangan fishing dan serangan

smishing. Serangan phishing melalui pesan verbal, sementara serangan smishing mengeksploitasi pesan SMS; Pesan teks yang disusupi dapat berisi alamat email dan situs web yang dapat mengarahkan pengguna yang tidak bersalah ke situs malware [10].

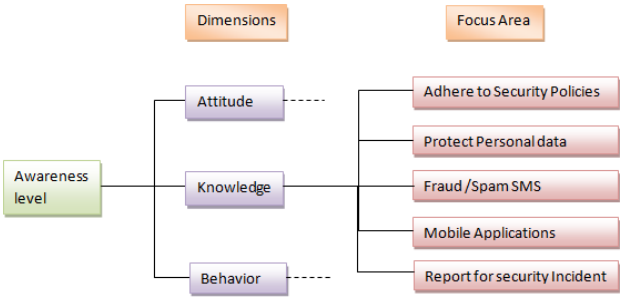
Seperti yang dijelaskan oleh banyak ahli, objek program kesadaran keamanan informasi berfokus pada karyawan dalam organisasi. Standar keamanan lainnya, seperti BMIS dari ISACA, mendefinisikan elemen orang dari manajemen keamanan informasi yang terdiri dari karyawan, kontraktor, vendor, dan penyedia layanan [1]. Sementara itu, peneliti juga mendefinisikan bahwa orang-orang utama dalam BMIS adalah mereka yang dipekerjakan dalam organisasi [11]. Selain itu, ISO27001 menyatakan bahwa orang-orang yang bekerja di bawah aturan organisasi harus menyadari keamanan informasi; dan semua karyawan organisasi serta kontraktor harus menerima pendidikan dan pelatihan kesadaran yang tepat dan pembaruan rutin dalam kebijakan dan prosedur organisasi yang terhubung ke fungsi pekerjaan mereka [12].

Dalam penelitian ini, konsumen dilibatkan sebagai elemen people dalam manajemen keamanan informasi. Konsumen dari beberapa organisasi juga memiliki akses ke jaringan komunikasi yang berarti mereka dapat memperoleh beberapa informasi organisasi. Seperti yang dikatakan Peltier, "PemilikS ystem memiliki tanggung jawab untuk berbagi pengetahuan yang sesuai tentang keberadaan dan tingkat umum langkah-langkah pengendalian sehingga pengguna lain dapat yakin bahwa sistem ini cukup aman" [13]. Selain itu, sebagaimana dinyatakan dalam BS ISO 27001, kontrol deteksi, pencegahan, dan pemulihan untuk melindungi dari malware harus diimplementasikan dan dikombinasikan dengan kesadaran pengguna yang appropiate [12]. Sekitar 40% pengguna jejaring sosial diserang oleh malware; dan pada bulan Desember 2010, salah satu botnet android pertama (disebut Gemini) ditemukan dan kode dibungkus di dalam aplikasi android yang sah yang pengembangnya tidak menyadari menyebarkan malware. Sekali lagi pada Maret 2011, Google menemukan botnet yang disebut "droiddream" [10]. "Sangat penting untuk menjaga masyarakat menyadari ancaman keamanan dan mendidik mereka untuk menggunakan praktik yang baik untuk mendapatkan keamanan yang lebih besar" (Al-Shehri) [9]. Terakhir, penelitian ini mengusulkan pengukuran kesadaran keamanan informasi dari konsumen penyedia telekomunikasi, khususnya pengguna handphone android. Dengan mengetahui tingkat kesadaran dari konsumen, organisasi dapat menetapkan kebijakan dan prosedur keamanan yang tepat untuk memberikan perlindungan yang lebih baik bagi konsumennya.

Tinjauan Pustaka

Penelitian ini dilakukan dengan menggunakan Kruger & Kerney Model [4]. Ini mengadaptasi teori psikologi sosial sebagai alat dengan mengusulkan tiga komponen untuk mengukur cara yang menguntungkan atau tidak menguntungkan untuk objek tertentu; ini adalah kognisi, pengaruh, dan perilaku [2]. Komponen-komponen itu digunakan untuk mengembangkan tiga dimensi yang setara yang dikenal sebagai pengetahuan (apa yang diketahui seseorang), sikap (bagaimana perasaan mereka tentang topik), dan perilaku (apa yang mereka lakukan) [1]. Masing-masing dimensi ini kemudian dibagi menjadi lima bidang fokus: (a) mematuhi kebijakan keamanan, (b) melindungi data pribadi, (c) penipuan/SMS spam, (d)

aplikasi seluler, dan (e) melaporkan insiden keamanan. Di bawah ini adalah metode yang diusulkan diadopsi dari model Kruger & Kerney.



Gambar 1. Kerangka Kerja Pengukuran Kesadaran Keamanan Informasi

Lima bidang fokus diekstraksi dari teori, fakta dan fenomena tentang keamanan informasi di Indonesia terkait sektor telekomunikasi. Selain itu, area didefinisikan oleh seorang pakar keamanan informasi dalam penyediaan telekomunikasi (auditor ISO 27000). Ada dua masalah yang disebutkan oleh ahli: (a) mematuhi kebijakan keamanan, dan (b) melaporkan insiden keamanan. Poin pertama kesadaran dalam ISO 27001:2013 menyatakan bahwa "orang yang melakukan pekerjaan di bawah kendali organisasi harus mengetahui kebijakan keamanan informasi" [12]. Itulah alasan mengapa kebijakan keamanan sebagai aspek mendasar dalam pengelolaan keamanan informasi harus dibahas sebagai salah satu bidang fokus.
Area fokus berikutnya adalah melindungi data pribadi. Sekarang, seperti yang tertulis dalam pengantar, orang menyimpan banyak informasi di handphone android, termasuk data pribadi dan rahasia. Mereka menggunakan handphone android tidak hanya untuk sms dan melakukan panggilan telepon, tetapi juga untuk melakukan bisnis dan banyak tujuan lainnya. Kami menempatkan area perlindungan data pribadi untuk dianalisis dalam penelitian ini.

Metodologi Penelitian

Penelitian ini menggunakan metode kuantatif di mana data dikumpulkan menggunakan kuesioner. Tiga puluh pertanyaan dirancang untuk menguji pengetahuan, sikap, dan perilaku mengenai lima bidang fokus utama. Setiap area fokus di setiap dimensi memiliki dua pertanyaan. Beberapa pertanyaan dijawab pada skala 3 poin-benar, tidak tahu dan salah (dimensi sikap dan pengetahuan), sementara yang lain hanya membutuhkan respons yang benar atau salah (dimensi perilaku), lihat contoh pertanyaan di Tabel 1. Kuesioner didistribusikan secara online.

Tabel 1. Contoh Pertanyaan

Untuk menguji	Jawaban	Pertanyaan
Pengetahuan	Untuk melindungi ponsel cerdas saya dari malware / virus jadi saya harus menginstal antivirus.	Benar, Tidak Tahu, Salah
Sikap	yang saya sadari untuk melindungi ponsel cerdas saya dari virus / malware jadi saya harus menginstal antivirus.	Benar, Tidak Tahu, Salah
Perilaku	saya menginstal antivirus untuk melindungi handphone android saya dari virus / malware yang dapat menyebabkan kerusakan handphone android saya.	Benar, Salah

Analisis data digunakan sebagai metode deskriptif. Metode ini menjelaskan atau memberikan gambaran umum tentang objek yang sedang dipelajari melalui data sampel atau populasi apa adanya, tanpa melakukan analisis, dan membuat kesimpulan yang berlaku untuk umum [14]. Populasi penelitian ini adalah orang-orang yang menggunakan handphone android dan layanan telekomunikasi dari penyedia telekomunikasi Indonesia. Untuk menentukan sampel, penelitian ini menggunakan pengambilan sampel non-probabilitas dengan teknik sampel purposif.

Variabel operasional dalam penelitian ini terdiri dari tiga dimensi, yaitu pengetahuan (apa yang mereka ketahui tentang topik ini?), sikap (bagaimana perasaan mereka tentang topik ini?), dan perilaku (apa yang mereka lakukan?). Setiap dimensi memiliki lima area fokus; mematuhi kebijakan keamanan, melindungi data pribadi, SMS penipuan/spam, aplikasi seluler, dan melaporkan insiden keamanan. Setiap area fokus memiliki indikator, misalnya dalam melindungi data pribadi, indikator menggunakan kata sandi di ponsel cerdas dan keluar dari akun mereka setelah selesai. Untuk menguji validitas setiap item dalam kuesioner, kami menggunakan korelasi Pearson Product Moment di mana setiap item yang memiliki koefisien korelasi sama atau lebih dari 0,3 valid. Untuk pengujian keandalan kami menggunakan metode Alpha Cronbach, di mana koefisien harus sama atau lebih dari 0,5.

Skala kesadaran ditentukan menggunakan proses hierarki analitik (AHP). Pendekatan AHP memanfaatkan perbandingan pasangan untuk memberikan evaluasi subjektif terhadap faktor-faktor berdasarkan penilaian dan pendapat profesional manajemen [3]. Skor untuk setiap area fokus per dimensi dihitung dan kemudian dinormalisasi ke jumlah satu. Skor total, v (a), ditentukan dengan menggunakan rumus di bawah ini [4].

Setiap dimensi dan area fokus memiliki bobot yang akan digunakan dalam komputasi skor kesadaran total. Bobot tersebut didefinisikan dalam Tabel 2 dan Tabel 3 sebagai berikut.

Tabel 2. Skor Pembobotan Untuk Dimensions

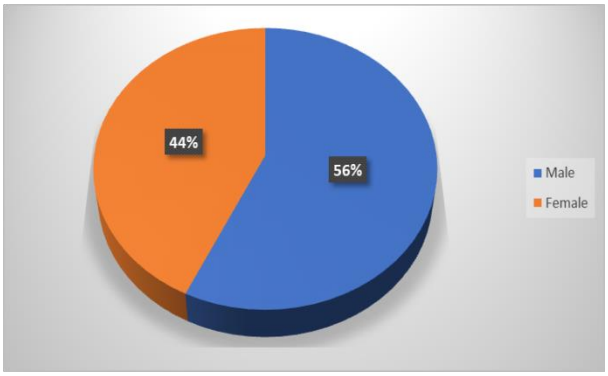
Dimensions	Pembobotan
Perilaku	20
Pengetahuan	30
Sikap	50

Tabel 3. Skor Pembobotan Untuk Area Fokus

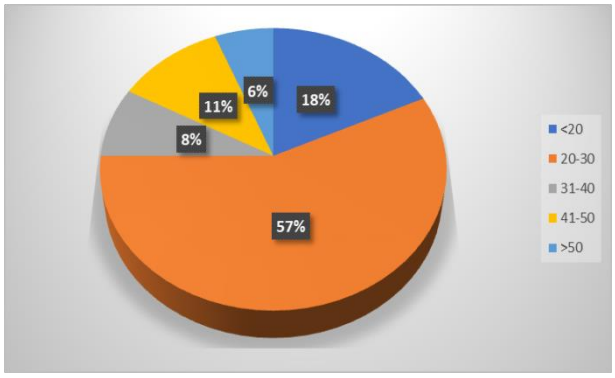
Area Fokus	Pembobotan
Mematuhi kebijakan keamanan	30
Lindungi data pribadi	20
Penipuan / spam SMS	20
Aplikasi Seluler	20
Laporan untuk Insiden Keamanan	20

Hasil dan Pembahasan

Survei dilakukan selama sekitar tiga minggu, dari tanggal 22 Desember 2021 hingga 12 Januari 2022. Jumlah responden adalah 107 pengguna dari beberapa program studi yang ada di Universitas Malikussaleh, Lhokseumawe; Informatika (63%), system Informasi (18%), Teknik Elektro (6%), Teknik Industri (4%) dan prodi lain (9%). Perempuan yang menggunakan handphone android dalam survei ini adalah 44% dan laki-laki 56% (Gambar 2). Berdasarkan rentang usia (3), mayoritas responden (57%) berasal dari kelompok usia 20-30 tahun kemudian diikuti oleh kelompok usia di bawah 20 tahun (18%), 41-50 tahun (11%), 31-40 (8%) dan berusia di atas 50 tahun (6%).

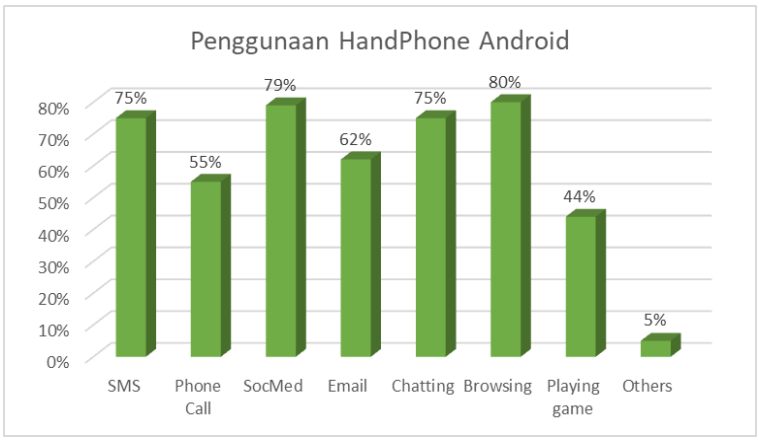


Gambar 2. Karakteristik terpusat berdasarkan jenis kelamin



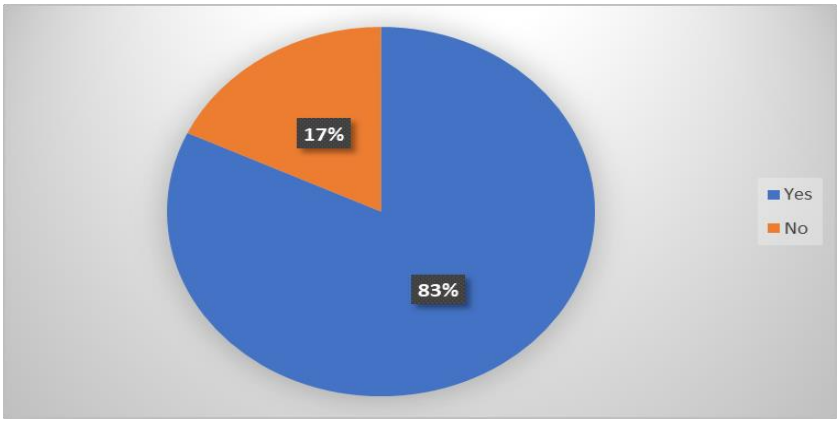
Gambar 3. Karakteristik terpusat berdasarkan rentang usia

Mengenai penggunaan handphone android oleh repondents, sebagian besar responden menggunakan handphone android untuk browsing (80%), media sosial (79%),SMS (75%) dan email (62%). Namun hanya beberapa pengguna yang menggunakan smartpohe untuk panggilan telepon (55%), bermain game (44%) dan lainnya (5%). Lainnya termasuk navigasi, catatan untuk kuliah, e-banking, dan aplikasi produktivitas. Penggunaan ini cocok dengan tren bahwa penggunaan internet atau data meningkat dan penggunaan panggilan telepon menurun. Hal ini dapat dilihat pada grafik pada Gambar 4.

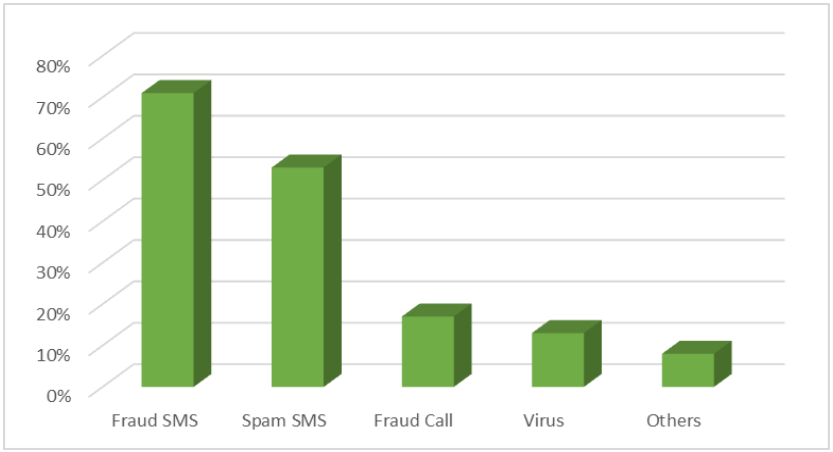


Gambar 4. Penggunaan handphone android

Mengenai pengalaman pelanggaran keamanan informasi berdasarkan survei, sebagian besar responden memiliki pengalaman, sekitar 83% dan mereka yang tidak memiliki pengalaman keamanan sekitar 17%. Rincian jumlah yang mengalami pelanggaran keamanan adalah sebagai berikut; penipuan SMS (71%), SMS spam (53%), panggilan penipuan (17%), virus (13%) dan lainnya (8%). Grafik seperti yang ditunjukkan pada Gambar 5 dan Gambar 6.



Gambar 5. Pengalaman Pelanggaran Keamanan Informasi



Gambar 6. Ancaman Keamanan Informasi

Skor hasil dari setiap area fokus dan dimensi kemudian dikelompokkan sebagai kriteria kesadaran dalam Tabel 4. Nilai interval dari kriteria tersebut didasarkan pada nilai garis kontinum di mana skor maksimum adalah 100% dan skor minimum adalah 33,33%. Setiap kriteria juga menunjukkan apakah rencana tindakan untuk perbaikan diperlukan atau tidak.

Tabel 4. Kriteria Kesadaran

Kriteria / Tingkat	Nilai (%)	Rencana Aksi
Bagus	77,78 - 100	Tidak perlu bertindak
Rata-rata	55,56 - 77,77	Tindakan berpotensi diperlukan
Miskin	33,33 - 55,55	Tindakan diperlukan

Tingkat kesadaran (lihat angka 6) digunakan untuk mempresentasikan hasil dan temuan proyek. Kode warna dapat memberikan informasi langsung tentang area mana yang safisfactory, harus dipantau, atau di mana tindakan harus diambil untuk perbaikan (tidak memuaskan). Jadi dengan kode warna, kita dapat melakukan dimensi atau area fokus mana yang harus diambil untuk tindakan untuk perbaikan dalam rangka meningkatkan tingkat kesadaran keamanan informasi.

Dari tingkat kesadaran keamanan informasi, kita dapat melihat bahwa:

- Tingkat kesadaran keseluruhan diukur sebagai 80%. Hal ini menunjukkan bahwa tingkat kesadaran **bagus**.
- Tingkat kesadaran untuk dimensi pengetahuan dan sikap yang **baik**, tetapi **memuaskan** untuk perilaku.
- Tingkat kesadaran total untuk area fokus yang mematuhi kebijakan keamanan, melindungi data pribadi dan SMS penipuan / spam **baik**. Namun tingkat kesadaran total untuk area aplikasi seluler dan melaporkan insiden keamanan **rata-rata** .

Hasil yang dirangkum dari tingkat kesadaran keamanan informasi menunjukkan bahwa area fokus berikut akan memerlukan tindakan potensial (tingkat rata-rata / memuaskan):

Mematuhi kebijakan keamanan

Dimensi perilaku masih pada tingkat yang memuaskan (75%). Berdasarkan pertanyaan yang diajukan, beberapa responden mungkin jarang membaca informasi tentang kebijakan keamanan saat mereka menginstal aplikasi dan mereka juga jarang mematuhi informasi tentang kebijakan keamanan. Ini mungkin memakan waktu lama untuk membaca semua item dalam kebijakan keamanan saat menginstal aplikasi baru atau membuat akun untuk layanan di media sosial, misalnya facebook, email, twitter dan sebagainya.

Alikasi seluler dengan hati-hati

Kedua pengetahuan (76%) dan perilaku (61%) dimensi harus menerima perhatian dalam hal pengetahuan dan perilaku. Berdasarkan pertanyaan yang diajukan, pengguna tidak menginstal antivirus untuk melindungi handphone android mereka dari virus atau malware yang dapat merusak handphone android mereka seperti yang dijelaskan dalam pengenalan. Selain itu mereka tidak memperbarui aplikasi antivirus secara teratur. Selain itu, rendahnya tingkat perilaku mungkin disebabkan oleh kurangnya pengetahuan tentang antivirus itu sendiri.

Melaporkan insiden keamanan

Untuk mencapai tingkat kesadaran yang tinggi, dimensi perilaku harus menerima lebih banyak perhatian. Dalam hal melaporkan insiden keamanan, mereka jarang melapor ke pusat panggilan mengeluh jika nomor telepon atau akun mereka dari media sosial (twitter, facebook, gmail, yahoo dll.) telah mengalami pelanggaran keamanan. Selain itu, mereka jarang melapor ke pusat panggilan operator telekomunikasi mengenai penipuan atau SMS spam.

Tabel 5. Tingkat kesadaran keamanan informasi

Area Fokus	pengetahuan (30)	sikap (20)	perilaku (50)	Total Kesadaran
Mematuhi kebijakan keamanan (20)	92	86	75	83
Melindungi data pribadi (20)	91	96	82	88
Premium/spam SMS (20)	92	88	84	86
Aplikasi Seluler (20)	76	82	61	72
Laporan untuk Insiden Keamanan (20)	81	89	64	75
Total Awareness/dimensions	86,4	88,2	73,2	80,8

Berdasarkan penjelasan di atas, disadari bahwa pengetahuan dan sikap ada dalam tingkat kesadaran keamanan informasi yang baik. Namun, dimensi perilaku masih pada tingkat yang memuaskan. Ini berarti bahwa meskipun mereka tahu tentang mematuhi kebijakan keamanan dan melaporkan insiden keamanan, mereka tidak melakukan seperti yang mereka ketahui dalam penggunaan handphone android. Ada beberapa alasan mengapa hal ini terjadi, misalnya dibutuhkan waktu lama jika mereka membaca semua item dalam kebijakan keamanan atau melaporkan insiden keamanan; mungkin, mereka tidak punya waktu untuk melaporkan masalahnya atau mereka menyelesaikan masalahnya. Dalam kasus area aplikasi seluler, dimensi sikap baik tetapi pengetahuan dan dimensi perilaku tingkat memuaskan. Ini berarti

bahwa karena kurangnya pengetahuan, pengguna tidak bertindak seperti yang diperlukan kebijakan.
Membandingkan penelitian kami dengan penelitian lain (Kruger's) [4] area fokusnya sedikit berbeda. Dalam jurnal ini, survei objek adalah mahasiswa Universitas Malikussaleh pengguna handphone android tetapi dalam jurnal Kruger, objek tersebut adalah karyawan perusahaan tambang emas internasional. Namun, dimensi, pembobotan, dan kriteria dalam jurnal ini sama dengan dalam jurnal Kruger.
Mengenai ancaman keamanan informasi (Gambar 5) dan hasil tingkat kesadaran keamanan informasi (Gambar 6), tampaknya ada kontradiksi antara pengalaman ancaman keamanan informasi dengan hasil tingkat kesadaran bahwa pengalaman ancaman SMS penipuan / spam tinggi tetapi tingkat kesadaran keamanan baik. Ini mungkin disebabkan oleh kesalahpahaman tentang penipuan / SPAM SMS di mana pertanyaannya adalah bahwa jika pengguna menerima pengumuman tentang menjadi pemenang hadiah dari satu penyedia atau orang lain, ia harus menghubungi pusat panggilan hukum penyedia untuk memeriksa validitas pengumuman. Selanjutnya, dari SMS tersebut terdapat informasi mengenai URL salah satu provider (sebenarnya ini adalah URL palsu) sehingga informasi sensitif pengguna dapat bocor.
Dalam hal area fokus aplikasi seluler jelas dipahami bahwa ada hubungan positif antara pengalaman ancaman keamanan informasi (Gambar 6) dengan hasil tingkat kesadaran (Gambar 7) bahwa pengalaman ancaman virus tinggi dan tingkat kesadaran keamanan rata-rata (perlu potensi peningkatan). Ini mungkin disebabkan oleh menggunakan atau menginstal aplikasi baru yang sebenarnya adalah virus sehingga ini dapat merusak (malfungsi) handphone android pengguna.

Kesimpulan

Berdasarkan penelitian kami, dinyatakan bahwa tingkat kesadaran keamanan bagi pengguna handphone android di Universitas Malikussaleh masih pada tingkat baik. Hal ini ditunjukkan dengan jumlah total kesadaran yaitu sekitar 80% meskipun ada beberapa bidang fokus yang harus diperbaiki agar memiliki potensi peningkatan. Dalam dimensi perilaku, yang harus diperbaiki adalah aplikasi seluler yang digunakan, melaporkan insiden keamanan dan mematuhi kebijakan keamanan. Sementara dalam dimensi pengetahuan, penggunaan aplikasi mobile yang harus ditingkatkan. Namun dalam dimensi sikap, semua area fokus berada pada tingkat yang baik.
Dengan menerapkan program kesadaran keamanan informasi untuk pengguna handphone android di Universitas Malikussaleh, diharapkan mereka memahami tentang keamanan dan menjaga informasi mereka dalam penggunaan handphone android untuk email, layanan di media sosial, SMS, chatting dll. Program kesadaran keamanan ini penting karena jumlah pengguna handphone android selalu meningkat setiaap tahun dan mereka menggunakannya untuk banyak keperluan.
Jika kesadaran pengguna baik dan ancaman keamanan informasi masih tinggi, mungkin ada faktor lain yang menyebabkannya. Oleh karena itu, untuk penelitian selanjutnya, dapat dikembangkan untuk menganalisis faktor-faktor penyebab mengapa pelanggaran keamanan informasi kepada pengguna handphone android masih relatif tinggi, terutama penipuan/SPAM SMS.

Daftar Pustaka

[1] Sari PK. A Concept of Information Security Management for Higher Education. International Conference on Technology and Operation Management, 3rd. Bandung. 2012: 469-477.

[2] Kruger H, and et al. A vocabulary Test to Assess Information Security Awareness. South African Information Security Multi-conference in Port Elizabeth, South Africa. 2010.

[3] Zhao J, Zhou Y, Shuo L. A Situation Awareness Model of System Saurvivability Based on Variable Fuzzy Set. TELKOMNIKA. 2012; 10(8): 2239-2246.

[4] Kruger HA, Kearney WD. A Protoype for Assessing Information Security Awareness. Elsevier Journal: Computers & Security. 2006; 25: 289-296.

[5] Symantec. Information Security Threat Reports. Symantec Corporation. 2013; 18.

[6] IDCERT. Laporan Dwi Bulan II 2013. Indonesia Computer Emergency Response Team. 2013.

[7] IDCERT. ID-CERT Annual Report 2012. Indonesia Computer Emergency Response Team. 2012.

[8] Shabech H, Jeyanthi N, Iyengar N.Ch.S.N. A study on security Threats in Cloud. International Jouarnal of Cloud Computing and Services Science (IJ-CLOSER). 2012; 1(3): 84-88.

[9] Al-Sehri Y. Information Security Awareness and Culture. British Journal of Arts and Social Sciences. 2012; 6(1): 61-69

[10] Laudon KC, Traver CG. E-Commerce 2012: Business, Technology, Society. England. Pearson Education Limited. 2012.

[11] ISACA. Business Model for Information Security. USA. 2010.

[12] British Standard Institution. ISO/IEC 27001:2013 Information Tecnology-Security Techniques- Information Security Management Systems-Requirements. Switzerland. BSI Standard Limited. 2013.

[13] Peltier, Thomas R. Information Security Fundamentals, Second Edition. Boca Raton. CRC Press. 2014.

[14] Sugiyono. Statistik Untuk Penelitian. Bandung. Alfa Beta. 2009.