

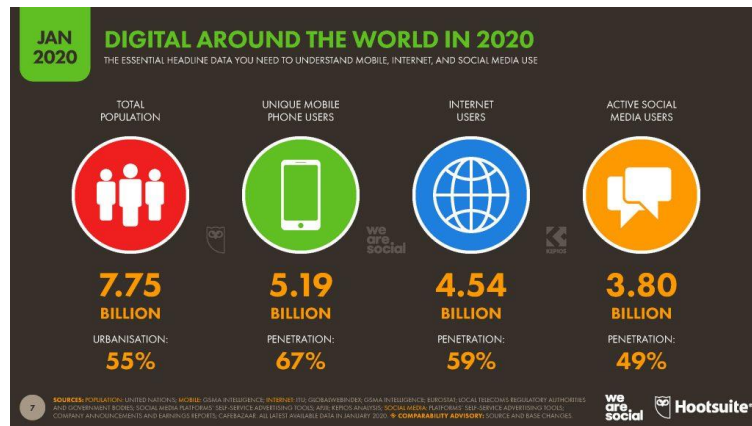
BAB I

PENDAHULUAN

1.1. Gambaran Umum Objek Penelitian

Objek Penelitian yang akan diteliti dalam skripsi ini adalah pengguna *smartphone*. *Smartphone* adalah telepon seluler yang bekerja pada sistem operasi (Gaurav & Manjusha, 2017) yang memungkinkan pengguna untuk menginstal dan menjalankan aplikasi yang lebih canggih berdasarkan platform tertentu. (Jeon, Kim, Lee, & Won, 2011). *Smartphone* menjadi semakin diperlukan dalam kehidupan sehari-hari dan menawarkan berbagai macam aplikasi seluler untuk tujuan informasi, komunikasi, pendidikan, dan hiburan. Ponsel cerdas biasanya memiliki layar sentuh, akses Internet seluler melalui Wi-Fi atau jaringan seluler, kemampuan untuk memasang aplikasi ponsel cerdas, dan fungsi lain seperti pemutar media, kamera digital, dan navigasi berbasis GPS. (Haug, Castro, Kwon, Kowatsch, & Schaub, 2015).

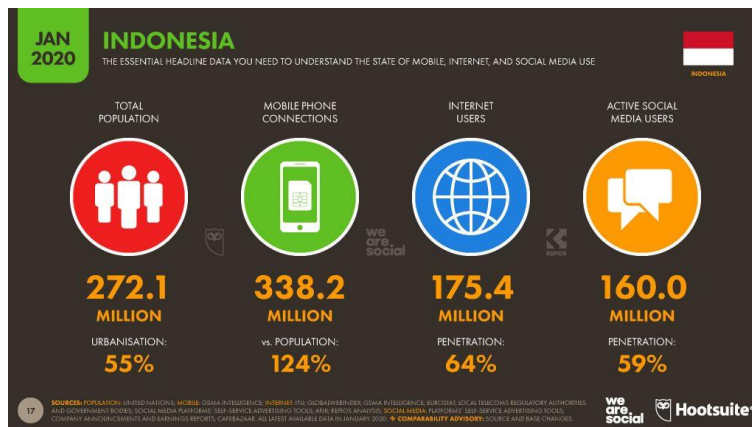
Fasilitas yang ada pada *smartphone* tidak hanya untuk telepon dan sms saja. *Smartphone* juga dapat digunakan untuk menjadi media hiburan dan juga tempat untuk menyalurkan hobi seseorang. Selain itu *smartphone* dapat dijadikan sarana untuk menjalankan bisnis online dan dapat menjadi alat untuk menyimpan berbagai macam data. (Daeng, Mewengkang, & Kalesaran, 2017). Seperti halnya pada komputer, *Smartphone* memiliki sistem operasi yang bekerja dalam menyelesaikan atau memenuhi permintaan dari pengguna. Diantaranya yaitu Android, iOS, Windows Mobile, Symbian, Blackberry, dan lain-lain. (Arnomo & Hendra, 2019).



Gambar 1. 1 Digital Around The World In 2020

Sumber : <https://wearesocial.com/digital-2020>

Berdasarkan hasil survey Hootsuite, dapat dilihat dari **Gambar 1.1**, pada tahun 2020 jumlah pengguna *mobile phone* sebanyak 5,19 milyar dari 7,750 milyar banyaknya populasi. Hootsuite juga menerangkan bahwa pengguna *mobile phone* di Indonesia sebanyak 338,2x juta, dapat dilihat pada **Gambar 1.2**.



Gambar 1. 2 Digital di Indonesia Pada Tahun 2020

Sumber : <https://wearesocial.com/>

1.2. Latar Belakang Penelitian

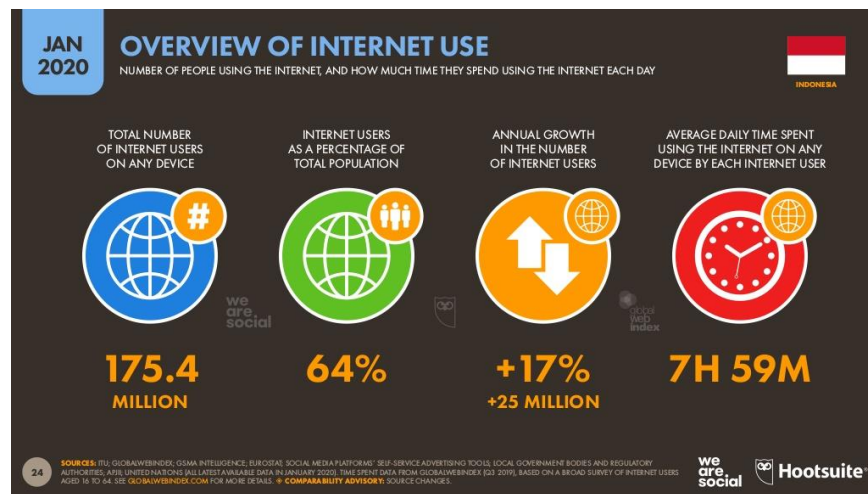
Saat ini teknologi semakin berkembang. Teknologi informasi dan komunikasi pun telah mengubah cara orang menghadapi aktivitas sehari-hari (Candiwan & Zafira, 2020). Perangkat teknologi seperti *handphone*, komputer, internet telah merevolusi kemampuan kita untuk menangkap informasi tentang dunia dan untuk berkomunikasi satu sama lain (Solove,

Rotenberg, & Schwartz, 2006). Salah satu bentuk dari kemajuan teknologi yaitu *smartphone*. (Nurhalimah, 2019). *Smartphone* memungkinkan berbagai fungsi seperti browsing internet, e-mail, Komunikasi suara, teks dan video serta penggunaan aplikasi yang diunduh menjadi terintegrasi ke dalam satu perangkat. (Hadjipanayis, Klonis, Abdel-Mannan, & Sutcliffe, 2016), selain itu *smartphone* dapat dijadikan sarana untuk menjalankan bisnis online dan dapat menjadi alat untuk menyimpan berbagai macam data. (Daeng, Mewengkang, & Kalesaran, 2017).

Smartphone memiliki berbagai manfaat yang bisa didapatkan, diantaranya yaitu komunikasi menjadi lebih lancar, dapat dijadikan sebagai media hiburan, dapat berselancar di dunia maya untuk mencari informasi, sebagai petunjuk arah dan menyimpan data yang berupa file dokumen, musik atau bahkan dalam bentuk video, foto dan lain-lain (Convert, 2020). Dengan manfaat dari penggunaan *smartphone*, saat ini orang banyak menyimpan informasi di *smartphone* mereka, termasuk data pribadi dan rahasia (Sari & Candiwan, 2014).

Meskipun *smartphone* memiliki banyak manfaat, *smartphone* juga dapat membawa dampak negatif yang memungkinkan terjadinya resiko pencurian data sehingga keamanan *smartphone* dalam menjaga data pribadi menjadi perhatian utama penggunanya (Sahiruddin, Riadi, & Sunardi, 2017). Meningkatnya serangan terhadap set informasi dan keberhasilan penyerangan kriminal menggambarkan kelemahan dan teknologi informasi saat ini dan kebutuhan untuk meningkatkan keamanan informasi (Solove, Rotenberg, & Schwartz, 2006).

Berdasarkan laporan We Are Social pada **Gambar 1.3**, penggunaan internet di Indonesia pada tahun 2020 ada 175,4 juta. Dibandingkan dengan tahun sebelumnya, terdapat kenaikan penggunaan internet sebanyak 17% atau 25 juta. Dengan persentase penggunaan internet sebesar 64% dari total populasi, yang berarti lebih dari setengah masyarakat Indonesia telah menggunakan internet.



Gambar 1.3 Overview Of Internet Use

Sumber : <https://wearesocial.com/>

Smartphone menggabungkan layanan internet dan ponsel (Cha & Seo, 2018). Dimana internet ini memerankan peran penting dalam kehidupan sehari-hari, keterlibatan internet dalam aktivitas sehari-hari membuat pengguna rentan terhadap serangan dunia maya contohnya *phising* (Namin, Hewett, Jones, & Pogrund, 2016). *Phising* merupakan tindakan kriminal dimana pelaku berupaya untuk mendapatkan informasi sensitif seperti *username* dan *password* (Radiansyah, Candiwan, & Priyadi, 2016). *Smartphone* menjadi target yang menarik bagi peretas, terutama dalam memasang kode berbahaya di perangkat korban dan mendapatkan akses tidak sah ke data sensitif pengguna (Alsaleh, Alomar, & Alarifi, 2017).

Menurut data dari Badan Siber dan Sandi Negara (BSSN), upaya serangan siber di Indonesia pada bulan januari hingga agustus 2020 tercatat hampir 190 juta, di mana BSSN mengungkapkan bahwa serangan siber meningkat lebih dari empat kali lipat dibandingkan periode yang sama tahun lalu yang tercatat di kisaran 39 juta (Salsabila, 2020). Banyak kasus terjadi di organisasi keamanan informasi mulai dari virus, social engineering, serangan DoS, hacker hingga pencurian data. Pelanggaran keamanan terus meningkat, baik dari segi jumlah insiden maupun kerugian finansial. (Candiwan, Sari, & Nurshabrina, 2016).

Salah satu metode populer untuk mendistribusikan malware adalah melalui lampiran di email. Untuk menghindari ancaman tersebut, pengguna harus menghindari mengklik link dalam email atau mendownload lampiran dari sumber yang tidak dikenal atau tidak tepercaya (Shah & Agarwal, 2020). Bagaimana pengguna individu menggunakan aplikasi tertentu sangat penting untuk keamanan informasi saat menggunakan ponsel cerdas (Zhang, Li, & Deng, 2017). Tindakan yang tepat dari pihak pengguna akan membantu mencegah insiden keamanan siber. Shah dan Argawal (2020) juga menjelaskan dengan Memindai ponsel cerdas secara teratur dengan aplikasi anti-virus / anti-malware dapat mengurangi kemungkinan infeksi malware. Praktik dan perilaku pencegahan tersebut dapat membantu pengguna melindungi kerahasiaan, integritas, dan ketersediaan informasi mereka di *smartphone* (Harris, Furnell, & Patten, 2014). Selain itu Souppaya dan Scarfone (2013) menjelaskan bahwa penggunaan utilitas tambahan yang tepat penting untuk keamanan informasi *smartphone*. *Smartphone* mudah dicuri, hilang, atau disusupi (Zhang, Li, & Deng, 2017). Ketika *smartphone* tidak sengaja hilang atau terinfeksi malware, data yang tersimpan di *smartphone* bisa diakses oleh pihak yang tidak berkepentingan (Imgraben, Engelbrecht, & Choo, 2014). Ini menunjukkan bahwa sangat penting untuk memiliki rencana pemulihan data dalam penggunaan *smartphone* untuk keamanan informasi (Zhang, Li, & Deng, 2017).

Maka dari itu keamanan aplikasi mobile perlu diperhatikan karena pengguna mungkin saja mengakses atau mengunduh aplikasi yang sudah ditanami virus/malware yang menjadi celah untuk melakukan serangan (Juhara, 2016). Pelanggaran keamanan dapat menimbulkan konsekuensi yang tidak menyenangkan seperti hilangnya produktivitas, pencurian aset informasi, waktu henti sistem, kerusakan infrastruktur TI, kerusakan reputasi organisasi dan organisasi dapat menghadapi tuntutan hukum, denda dan tindakan regulasi (Gangire, Veiga, & Herselman, 2020). Oleh karena itu, Pengelolaan keamanan sistem yang

baik dibutuhkan untuk mengantisipasi ancaman-ancaman yang mungkin terjadi (Chazar, 2015).

Berdasarkan uraian yang telah dikemukakan, maka peneliti tertarik untuk melihat bagaimana *security behaviour* pengguna *smartphone* di Indonesia dengan penelitian yang berjudul “Analisis Perilaku Keamanan Informasi Pada Pengguna *smartphone* di Indonesia”

1.3. Perumusan Masalah

Saat ini teknologi semakin berkembang, dan dinamika kehidupan pun semakin berkembang. Perangkat teknologi seperti *handphone*, komputer, internet telah merevolusi kemampuan kita untuk menangkap informasi tentang dunia dan untuk berkomunikasi satu sama lain (Solove, Rotenberg, & Schwartz, 2006). Salah satu bentuk dari kemajuan teknologi yaitu *smartphone*. *Smartphone* kini telah berkembang dengan fitur yang disesuaikan dengan zaman dan kebutuhan penggunanya. Tetapi dari perkembangan *smartphone* juga membawa dampak negatif yang memungkinkan terjadinya resiko pencurian data sehingga keamanan *smartphone* dalam menjaga data pribadi menjadi perhatian utama penggunanya (Sahiruddin, Riadi, & Sunardi, 2017).

Keamanan aplikasi mobile perlu diperhatikan karena pengguna mungkin saja mengakses atau mengunduh aplikasi yang sudah ditanami virus/malware yang menjadi celah untuk melakukan serangan (Juhara, 2016). Oleh karena itu, pengelolaan keamanan sistem yang baik dibutuhkan untuk mengantisipasi ancaman-ancaman yang mungkin terjadi (Chazar, 2015). Berdasarkan uraian yang telah dikemukakan, maka peneliti tertarik untuk melihat bagaimana *security behaviour* pengguna *smartphone* dalam media tersebut dengan penelitian yang berjudul “Analisis Perilaku Keamanan Informasi Pada Pengguna *smartphone* di Indonesia”

Rumusan masalah yang ingin diselesaikan dalam penelitian ini adalah :

1. Bagaimana *security behaviour (avoiding harmful behaviour)* pengguna *smartphone* di Indonesia berdasarkan demografi jenis

kelamin, generasi, latar belakang pendidikan, dan operasi sistem (OS) pengguna *smartphone*?

2. Bagaimana *security behaviour (Setting & Add-on Utilities)* pengguna *smartphone* di Indonesia berdasarkan demografi jenis kelamin, generasi, latar belakang pendidikan, dan operasi sistem (OS) pengguna *smartphone*?
3. Bagaimana *security behaviour (Preventive behaviour)* pengguna *smartphone* di Indonesia berdasarkan demografi jenis kelamin, generasi, latar belakang pendidikan, dan operasi sistem (OS) pengguna *smartphone*?
4. Bagaimana *security behaviour (Recovery data)* pengguna *smartphone* di Indonesia berdasarkan demografi jenis kelamin, generasi, latar belakang pendidikan, dan operasi sistem (OS) pengguna *smartphone*?
5. Apakah ada kesesuaian antara tingkat *motivation, ability* dan *threat awareness* dengan penerapan *security behaviour* pengguna *smartphone* di Indonesia?

1.4. Tujuan Penelitian

Sesuai dengan rumusan masalah diatas, penelitian ini bertujuan sebagai berikut :

1. Mengetahui *security behaviour (avoiding harmful behaviour)* pengguna *smartphone* di Indonesia berdasarkan jenis kelamin, generasi, latar belakang pendidikan, operasi sistem (OS) yang digunakan pengguna.
2. Mengetahui *security behaviour (Setting & Add-on Utilities)* pengguna *smartphone* di Indonesia berdasarkan jenis kelamin, generasi, latar belakang pendidikan, operasi sistem (OS) yang digunakan pengguna.
3. Mengetahui *security behaviour (Preventive behaviour)* pengguna *smartphone* di Indonesia berdasarkan jenis kelamin, generasi, latar belakang pendidikan, operasi sistem (OS) yang digunakan pengguna.

4. Mengetahui *security behaviour (Recovery data)* pengguna *smartphone* di Indonesia berdasarkan jenis kelamin, generasi, latar belakang pendidikan, operasi sistem (OS) yang digunakan pengguna.
5. Mengetahui tingkat *motivation, ability, dan cybersecurity threat awareness* pengguna *smartphone* di Indonesia.

1.5. Manfaat Penelitian

1.5.1. Manfaat Teoritis

Penelitian ini memaparkan bagaimana perilaku keamanan informasi saat menggunakan *smartphone* dengan mengukur tingkat kesadaran dari penggunanya terhadap keamanan sistem informasi tersebut. Hasil dari penelitian ini diharapkan dapat memberikan pengetahuan berupa informasi pada pengguna *smartphone* sebagai alat ukur dalam pengukuran kesadaran keamanan informasi dalam penggunaan *smartphone* dan dapat dijadikan rujukan penelitian berikutnya.

1.5.2. Manfaat Praktis

Hasil dari penelitian ini memiliki manfaat yang dapat memberikan pengetahuan serta masukan bagi pengguna *smartphone* di Indonesia. Selain itu penelitian ini diharapkan pengguna *smartphone* lebih menjaga data-data pengguna itu sendiri agar tidak disalahgunakan.

1.6. Sistematika Penulisan Tugas Akhir

Untuk mempermudah dalam memahami isi penelitian, maka penulis menjabarkan sistematika penulisan yang digunakan untuk memberikan gambaran mengenai penelitian terkait :

a. BAB I PENDAHULUAN

Bab ini merupakan penjelasan secara umum, ringkas dan padat yang menggambarkan dengan tepat isi penelitian. Isi bab ini meliputi: Gambaran Umum Objek penelitian, Latar Belakang Penelitian,

Perumusan Masalah, Tujuan Penelitian, Manfaat Penelitian, dan Sistematika Penulisan Tugas Akhir.

b. BAB II TINJAUAN PUSTAKA

Bab ini berisi teori dari umum sampai ke khusus, disertai penelitian terdahulu dan dilanjutkan dengan kerangka pemikiran penelitian yang diakhiri dengan hipotesis jika diperlukan.

c. BAB III METODE PENELITIAN

Bab ini menegaskan pendekatan, metode, dan teknik yang digunakan untuk mengumpulkan dan menganalisis temuan yang dapat menjawab masalah.

d. BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Hasil penelitian dan pembahasan diuraikan secara sistematis sesuai dengan perumusan masalah serta tujuan penelitian dan disajikan dalam sub judul tersendiri. Bab ini berisi dua bagian: bagian pertama menyajikan hasil penelitian dan bagian kedua menyajikan pembahasan atau analisis dari hasil penelitian. Setiap aspek pembahasan hendaknya dimulai dari hasil analisis data, kemudian diinterpretasikan dan selanjutnya diikuti oleh penarikan kesimpulan. Dalam pembahasan sebaiknya dibandingkan dengan penelitian sebelumnya atau landasan teoritis yang relevan.

e. BAB V KESIMPULAN DAN SARAN

Kesimpulan merupakan jawaban dari pertanyaan penelitian, kemudian menjadi saran yang berkaitan dengan manfaat penelitian.