BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Objek penelitian yang diambil oleh penulis dalam skripsi ini adalah pengguna *smartphone* Android.

Android adalah sebuah sistem operasi untuk perangkat mobile berbasis linux yang mencakup sistem operasi, middleware dan aplikasi. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka. Awalnya google Inc. membeli Android Inc, yang merupakan pendatang baru yang membuat peranti lunak untuk smartphone. Kemudian untuk mengembangkan android dibentuklah open handset alliance, konsorium dari 34 perushaan peranti keras, peranti lunak dan telekomunikasi termasuk, google, HTC, Intel, Motorola, Qualcomm, T-Mobile, Nvidia. (Safaat 2015:3)

Android didirikan di Palo Alto, California, pada bulan Oktober 2003 oleh Andy Rubin, Rich Miner, Nick Sears, dan Chris White untuk mengembangkan perangkat seluler pintar yang lebih sadar akan lokasi dan preferensi penggunanya. Tujuan awal pengembangan Android adalah untuk mengembangkan sebuah sistem operasi canggih yang diperuntukkan bagi kamera digital, namun karena pasar untuk perangkat tersebut tidak besar, Android lalu dialihkan ke pasar *smartphone* untuk menyaingi Symbian dan Windows Mobile.

Gambar 1. 1

Logo Android

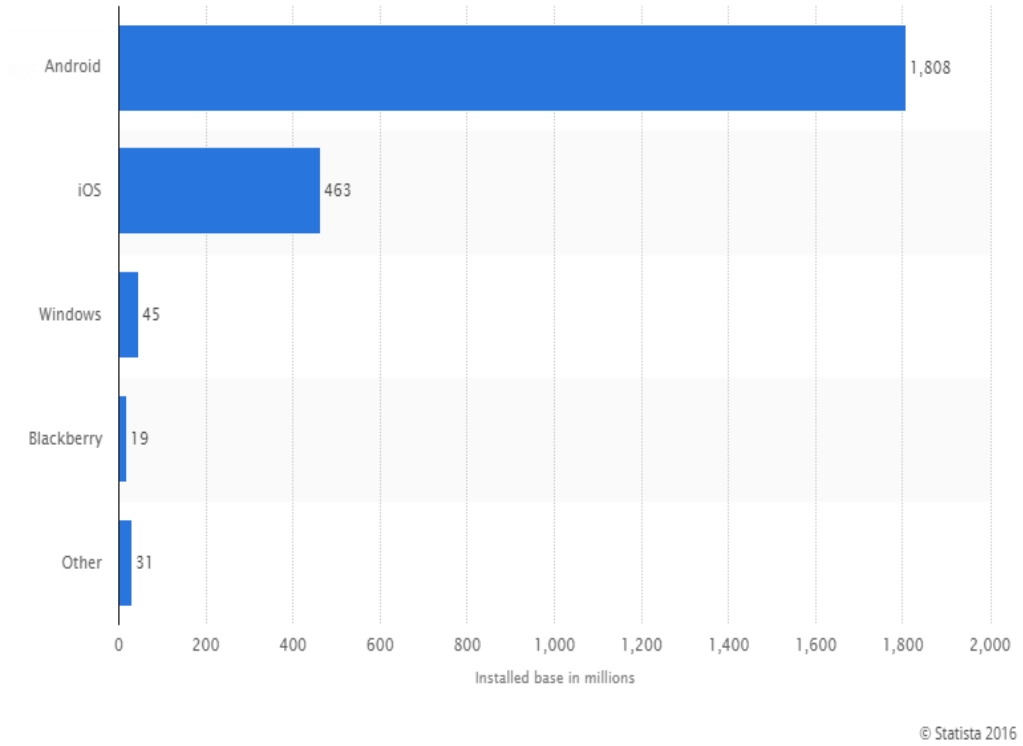
Sumber : www.android.com

Google mengakuisisi Android Inc. pada tanggal 17 Agustus 2005, menjadikannya sebagai anak perusahaan yang sepenuhnya dimiliki oleh Google. Sejak tahun 2008, Android secara bertahap telah melakukan sejumlah pembaruan untuk meningkatkan kinerja sistem operasi, menambahkan fitur baru, dan memperbaiki kesalahan yang terdapat pada versi sebelumnya. Setiap versi utama yang dirilis dinamakan secara alfabetis berdasarkan nama-nama makanan pencuci mulut atau cemilan bergula; misalnya, versi 1.5 bernama *Cupcake*, yang kemudian diikuti oleh versi 1.6 *Donut*. Versi terbaru adalah 6.0 *Marshmallow*, yang dirilis pada 19 Agustus 2015.

Android memiliki beberapa keamanan dalam sistem operasinya salah satunya adalah *sandbox*, sebuah area terisolasi yang tidak memiliki akses pada sistem, kecuali izin akses yang secara eksplisit diberikan oleh pengguna ketika memasang aplikasi. Sebelum memasang aplikasi, Play Store akan menampilkan semua izin yang diperlukan, misalnya: sebuah permainan perlu mengaktifkan getaran atau menyimpan data pada Kartu SD, tapi tidak perlu izin untuk membaca SMS atau mengakses buku telepon. Setelah meninjau izin tersebut, pengguna *smartphone* dapat memilih untuk menerima atau menolaknya, dan bisa memasang aplikasi hanya jika pengguna *smartphone* menerimanya. (Salbino 2014:9).

1.2 Latar Belakang Penelitian

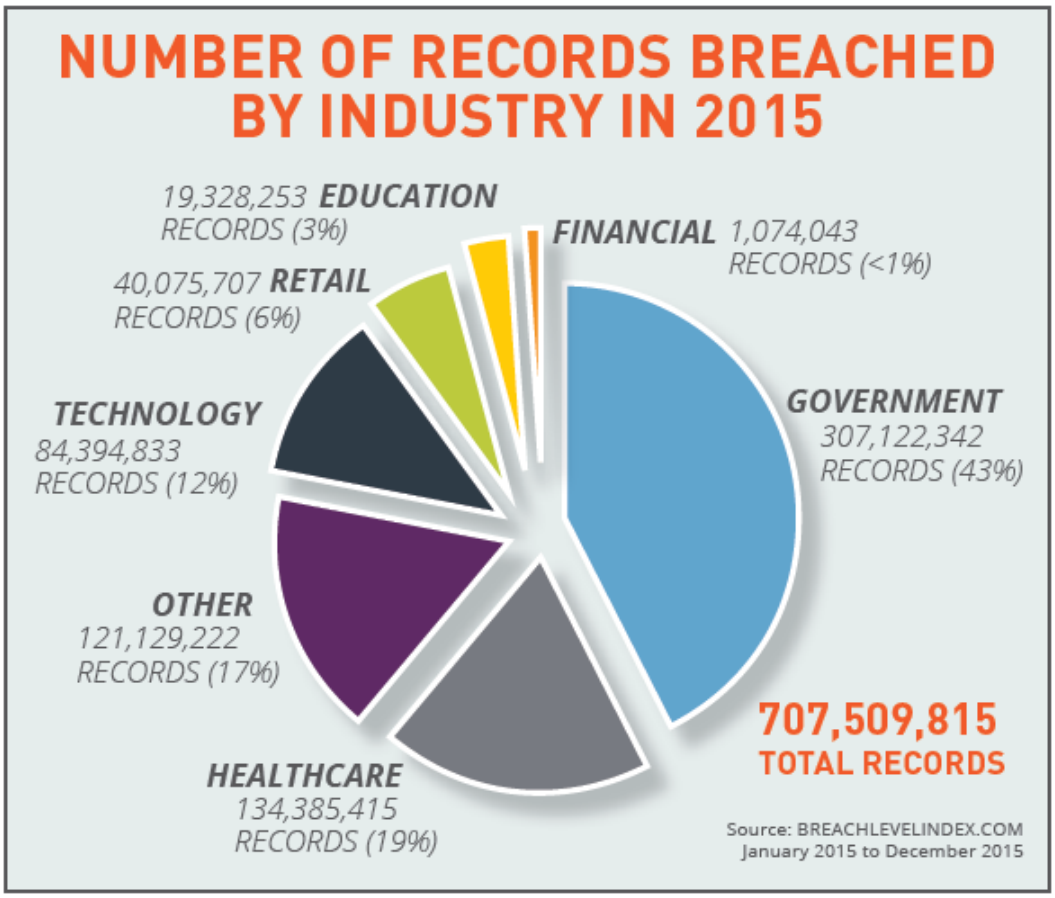
Di era teknologi informasi ini *smartphone* menjadi kebutuhan untuk bisa berkomunikasi dan berbagi informasi seperti mengirim SMS atau email, *entertainment*, media sosial tanpa mengkhawatirkan jarak dan waktu. Berbagai jenis *smartphone* dengan kelebihan OS (*operating system*) –nya masing-masing telah digunakan oleh setiap orang di seluruh penjuru dunia. Menurut data yang dilansir website statista di awal tahun 2016, Android merupakan *smartphone* terpopuler dengan jumlah pengguna terbanyak di dunia, yaitu sekitar 1,8 miliar. Diikuti sang pesaing Apple dengan iOSnya yaitu sekitar 463 juta penguuna, Windows dengan 45 juta pengguna, disusul Blackberry dengan jumlah pengguna sebanyak 19 juta, serta jenis *smartphone* lainnya dengan 31 juta pengguna.



Gambar 1.2
Urutan *Smartphone* Paling Populer di Dunia Tahun 2016
Sumber : www.statista.com

Dilansir oleh website techinasia pada bulan Januari tahun 2016, disebutkan bahwa jumlah pengguna dan penetrasi internet di Indonesia kini telah mencapai angka 88,1 juta. Disebutkan juga dalam website techinasia dari total populasi sebanyak 259.1 juta penduduk di Indonesia 43% nya menggunakan *smartphone* sebagai perangkat mereka. Di Indonesia berarti sekitar 111 juta orang yang menggunakan *smartphone* pada tahun 2016 dan akan terus meningkat seiring berjalannya waktu.

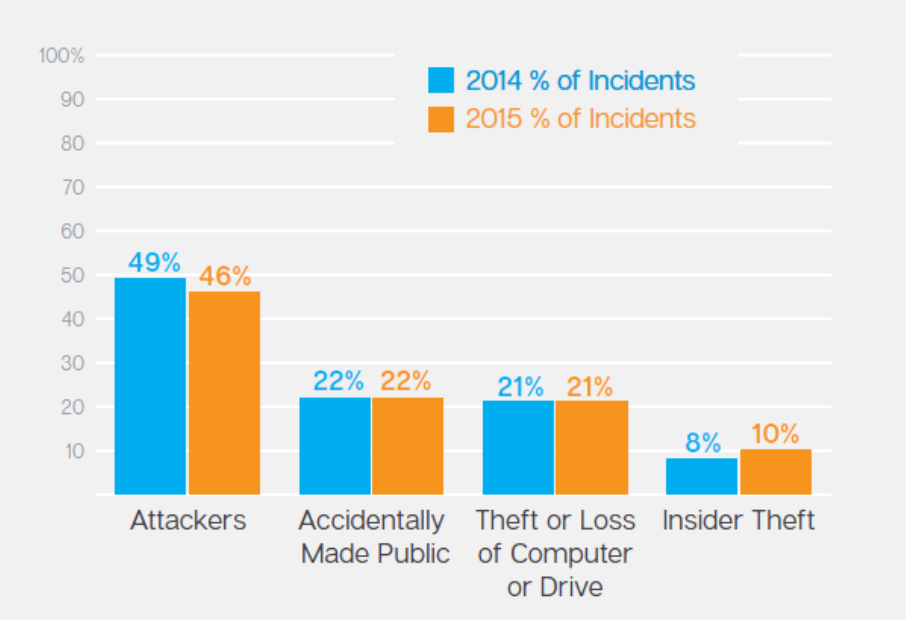
Menurut website statista pangsa pasar yang dimiliki oleh sistem operasi *mobile* di Indonesia di awal bulan Januari 2016 77,2% dimiliki oleh sistem operasi Android berarti sekitar 85.692.000 orang menggunakan *smartphone* Android dari total pengguna *smartphone* di Indonesia. Fenomena ini mungkin karena harga murahnya gadget dan layanan yang disediakan oleh penyedia telekomunikasi (Puspita, 2014).



Gambar 1.3
7 Sektor Industri Dengan Kebocoran Informasi Terbanyak Tahun 2015
Sumber : Gemalto

Dilansir Gemalto tahun 2015, sektor teknologi di peringkat keempat (12%) yang memiliki jumlah laporan pelanggaran sebanyak 84.394.833 laporan (top 7 sektor dengan jumlah laporan pelanggaran). Emergency Response Team Indonesia Computer (ID-CERT) telah melakukan survei, dengan beberapa responden dari penyedia telekomunikasi, yang 30,99% dari insiden dilaporkan dari bulan Januari sampai Februari 2015 adalah *spam*; 27.31% adalah Respon terhadap laporan yang masuk. 15.67% adalah hak kekayaan intelektual; 4,53% *spoofing/phising*; 3,98% *network incident* ; dan 3.18% adalah *malware*. Dilansir Symantec tahun 2014 jumlah jenis *malware* yang ditemukan dalam sistem operasi 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. Oleh karena itu, semua tindakan pencegahan untuk mengurangi insiden ini harus ditingkatkan dan diperkuat oleh penyedia layanan internet, termasuk industri telekomunikasi itu sendiri.

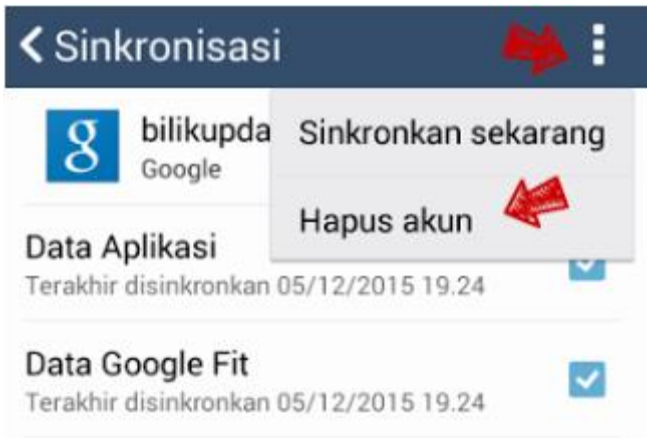


Gambar 1.4
Penyebab Terjadinya Pelanggaran Data
Sumber : symantec

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.

Android adalah sistem operasi besutan Google yang sengaja diciptakan untuk perangkat mobile, Kelebihan dari Android yakni dilengkapi dengan berbagai fitur serta aplikasi yang sangat canggih dan lengkap, terdapat juga toko aplikasi resmi dari Android untuk mendoenload berbagai game serta aplikasi. Adapun nama dari toko aplikasi Android tersebut adalah Play Store.

Walaupun Android memiliki banyak kelebihan tentu saja juga memiliki kekurangan antara lain ialah tidak ada opsi log out/sign out email di Android tanpa menghapus seluruh akun dari ponsel ataupun tablet hal ini menambah kerentanan terhadap pencurian data yang dapat dilakukan dengan mengambil data yang terdapat dalam email pengguna.



Gambar 1.5
Cara Hapus Akun Gmail di Smartphone Android
Sumber : kutazo.net

Menurut website *support.google.com* dikatakan bahwa pengguna *smartphone* dapat menghapus Akun Google -nya kapan saja, tetapi mungkin tidak selalu dapat memulihkannya, Inilah yang terjadi jika menghapus Akun Google pada *smartphone* , pengguna tidak dapat lagi menggunakan berikut ini:

- Layanan yang mengharuskan pengguna untuk masuk, seperti E-mail, Drive, dan Kalender
- Data terkait akun, termausk email, foto, dan catatan transaksi
- Langganan dan konten yang dibeli di YouTube, seperti film dan acara TV
- Konten yang pengguna beli di Google Play, seperti film, game, atau musik
- Informasi yang tersimpan di Chrome
- Username Gmail pengguna. Setelah menghapusnya, pengguna tidak dapat menggunakannya lagi nanti, dan tidak dapat membuat Akun Google baru dengan nama pengguna baru.

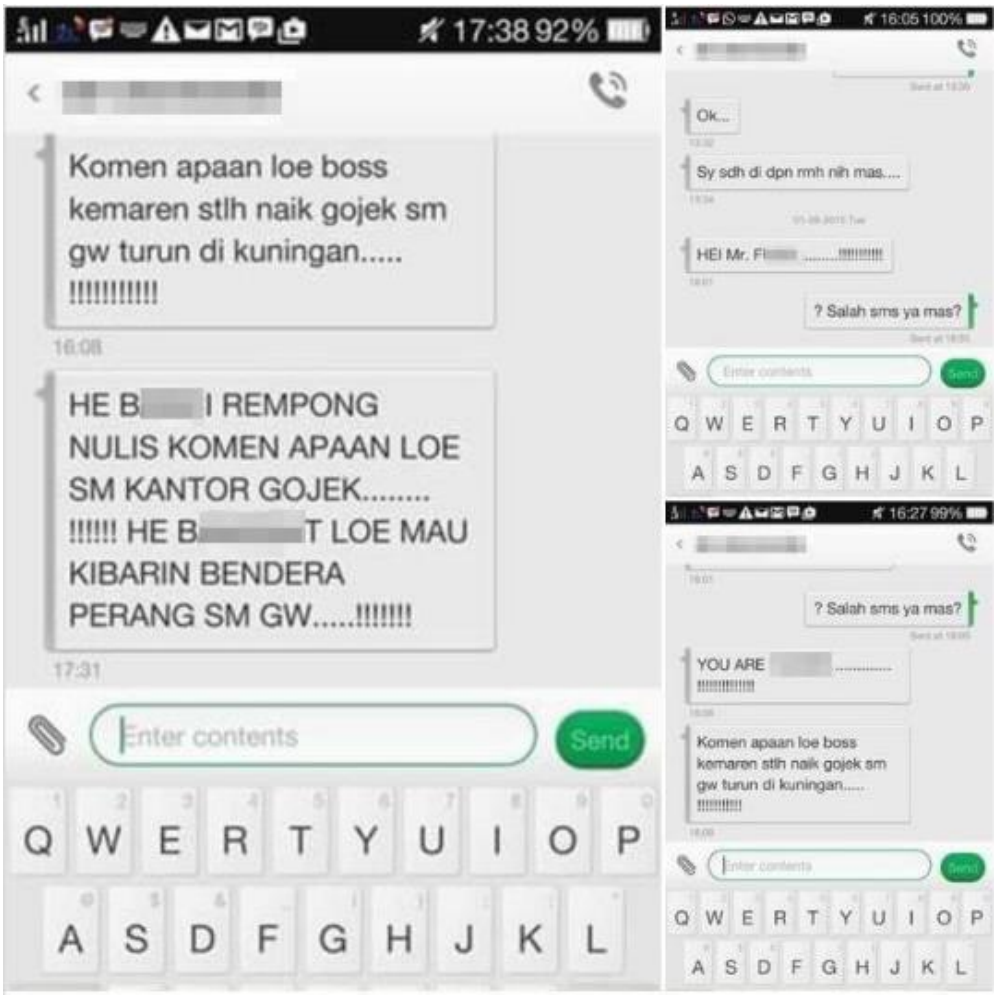
Sistem operasi Android memiliki berbagai macam aplikasi. Di dalamnya terdapat ribuan bahkan jutaan aplikasi yang dapat memenuhi kebutuhan bahkan memudahkan pekerjaan pengguna *smartphone*.

Berbgai aplikasi telah digunakan oleh banyak pengguna smartphone. Namun, selain merugikan keamanan informasi, saat ini tanpa diketahui oleh pengguna, ternyata tidak sedikit pembuat aplikasi yang merugikan privasi pengguna *smartphone*. Untuk menggunakan aplikasi pada OS ini, pengguna diwajibkan untuk menginstal aplikasi terlebih dahulu. Ketika proses instalasi akan berlangsung, pengguna diminta untuk memberikan izin akses terhadap *resource* tertentu yang diminta oleh aplikasi, tanpa menjelaskan mengapa resource tersebut dibutuhkan oleh aplikasi. Banyak pengguna yang tidak sadar/tidak tahu/masa bodoh dengan permintaan ini, sehingga pengguna *smartphone* akan mengizinkan untuk menginstal aplikasi (girindropringgodigdo 2015*)*.

Gambar 1.6
Hak Akses Aplikasi pada Smartphone Android
Sumber : girindropringgodigdo.net

Dari aturan seperti ini, para pembuat aplikasi dapat saja mensyaratkan pengguna untuk mengizinkan mereka (*developer*) untuk dapat mengakses *resource* yang krusial seperti penyimpanan, kontak, perpesanan, serta *resource* lainnya. Sayangnya, tidak sedikit pengguna yang tidak membaca *terms and conditions* ini dan langsung menginstal aplikasi yang mereka inginkan. Akibatnya, memang mereka dapat menggunakan aplikasi, namun di pihak *developer*, pun dapat mengakses data pengguna.

Di Indonesia sendiri terjadi beberapa pelanggaran privasi seperti yang dilansir oleh website techinasia (2015) pengendara Gojek itu mengirimkan SMS kepadanya berisi kemarahannya karena telah diberi *review* yang buruk.



Gambar 1.7
Pelanggaran Privasi yang Dilakukan Oleh Gojek
Sumber : id.techinasia.com

Menurut website aitinesia (2015) dijelaskan bagaimana alur pemesanan Go-Jek dan GrabBike dari awal hingga akhir. Pertama dimulai dengan memesan Go-Jek / GrabBike lewat aplikasi *mobile*, maka selanjutnya nama konsumen akan tercantum di smartphone pengendara Go-Jek / GrabBike, beserta rute pengantaran yang diinginkan. Setelah itu, pengendara Go-Jek / GrabBike dapat menghubungi nomor telepon yang konsumen gunakan di *smartphone* yang terdapat aplikasi Go-Jek / GrabBike untuk mengkonfirmasi titik jemput. Setelah itu, konsumen akan diantar ke rumah atau ke kantor, maka pengendara Go-jek / GrabBike juga akan mengetahui alamat rumah konsumen. Jadi dalam satu kali perjalanan saja, seorang pengendara Go-Jek / GrabBike sudah bisa mengetahui data-data Nama konsumen, Nomor Telepon konsumen, dan Alamat Rumah atau Kantor konsumen. Hal itu jelas merupakan sebuah pelanggaran privasi yang rentan disalahgunakan, dan akibatnya bisa jadi fatal.

Menurut situs Maxmanroe (2015) Kian hari smartphone menjadi sesuatu yang wajib bagi banyak orang, bahkan bisa dikatakan menjadi barang pribadi yang harus ada di manapun seseorang itu berada. Smartphone juga semakin canggih dengan spesifikasi yang semakin tinggi lagi, dengan harga yang sangat bervariasi. Begitu juga dalam hal teknologi keamanan, semua produsen *smartphone* terus mengembangkan keamanan tertinggi untuk menghindari privasi para konsumen dicuri oleh pihak yang tidak bertanggung jawab, yaitu *hacker. Hacker* tidak henti-hentinya menyerang segala jenis *smartphone*, termasuk Android. Banyak sekali cara yang dilakukan oleh para *hacker* untuk menyerang para pemilik smartphone Android dengan tujuan untuk mencuri data, untuk merusak sistem, dan lainnya.

Menurut Jofino (2016) ada empat macam penipuan yang biasa terjadi di smartphone Android, yaitu :

1. Penipuan Melalui Pesan di Email

   Penipuan melalui pesan yang dikirimkan ke email memang sudah banyak terjadi. Modus yang digunakan adalah berupa undangan ke sebuah acara ataupun memberikan promosi terhadap suatu produk maupun jasa. Biasanya, dalam email seperti ini korban harus menyertakan informasi

pribadi seperti nomor telepon, alamat, nomor jaminan sosial, tempat/tanggal lahir, bahkan hingga rincian keuangan kamu.

Selain itu, penipuan via email lainnya adalah korban akan diberitahu bahwa rekening bank telah dicuri dan perlu diverifikasi ulang. Kemudian, pesan tersebut akan mengarahkan kamu untuk memasukkan rincian *login* bank yang kamu gunakan, informasi pribadi atau sandi rahasia kamu ke link yang mereka berikan. Setelah kamu isi, penipuan itu barulah terjadi.

2. Aplikasi Palsu di Samrtphone Android

   Aplikasi yang terlihat dan berfungsi layaknya aplikasi resminya, tetapi sebenarnya aplikasi ini merupakan *malware* yang dapat mencuri informasi di smartphone Android. Aplikasi ini tidak hanya terjadi di file APK, namun beberapa aplikasi lainnya juga dapat ditemukan di Google Play. Contohnya adalah versi "eksklusif" dari WhatsApp yang disebut WhatsApp Gold. WhatsApp Gold merupakan aplikasi palsu. Ketika diunduh, smartphone Android dipastikan akan terinfeksi *malware*. Selain itu, aplikasi penipuan berbau WhatsApp lainnya adalah WhatsApp Plus.

3. Penipuan Berupa Dukungan Teknis

   Apa yang dimaksudkan adalah akan ada telepon dari seseorang yang mengatakan bahwa mereka dari pihak dukungan teknis dari penyedia layanan kartu SIM yang sedang digunakan atau dari perusahaan smartphone yang sedan digunakan. Dari situ lah penipu mencuri informasi pribadi kamu.

   Salah satu alasan paling kuat yang digunakan oleh si penipu adalah tentang 'ransomware'. Alibi dukungan teknis ini akan mengklaim bahwa smartphone Android telah terinfeksi virus dan juga mereka atau penipu akan mulai pura-pura membantu. Kemudian, diarahkan untuk membeli sesuatu dari situs palsu dan kembali mengorek informasi mengenai rincian kartu kredit kamu melalui telepon tersebut

4. Penipuan di Konter HP

   Salah satu masalah yang paling sering dihadapi oleh para pengguna smartphone Android di tanah air adalah, saat ponsel kamu rusak, terus kamu

bawa ke konter untuk diservis. Saat smartphone mengalami *error*, tentu saja kita akan membawanya ke konter handphone di sebuah mal ataupun konter-konter ponsel pinggir jalan. Dalam kondisi inilah yang paling tepat untuk para penipu melaksanakan aksinya. Mereka akan mengatakan bahwa smartphone Android mengalami beberapa masalah dan harus diperbaiki selama sekian hari, kemudian data pribadi kamu akan dikorek, bahkan *hardware* dari smartphone tersebut juga akan ditukar dengan kualitas yang lebih rendah.

Tabel 1. 1
Tabel Daftar Kasus Android (2013-2016)

No	Waktu	Peristiwa	Sumber
1	12/01/2016	Terdapat 13 aplikasi dilaporkan dihapus dari Google Play Store sebagai bagian dari rantai malware yang disebut Brain Test. Aplikasi berbahaya itu akan dapat menginstal perangkat Android dan akan mencoba mendapatkan akses root. Aplikasi tersebut juga akan membantu menginstal aplikasi yang terinfeksi malware lainnya pada perangkat yang sama tanpa sepengetahuan pemilik ponsel. Karena 13 aplikasi tersebut merupakan aplikasi permainan yang menarik, semakin besar peluang untuk diinstal oleh pengguna Android. Aplikasi yang terinfeksi tersebut mampu menciptakan ulasan palsu di Google Play Store, sehingga menarik pengguna Android untuk menginstalnya. Pasalnya, pada saat terdeteksi, aplikasi-aplikasi tersebut dalam proses menginstal aplikasi-aplikasi lain yang terinfeksi virus di berbagai unit lain. Sehingga, meskipun tidak terlihat, kerusakan handset yang	Muhammad (2016)

		terinfeksi malware bisa sangat besar. Contoh aplikasi nya adalah game cake blast, jump planet, Honey Comb, Crazy Jelly dll	
2	26/08/2013	Kaspersky Lab's mengungkapkan hasil monitoring spam selama Juli memperlihatkan target malware masih menyasar data personal pengguna. Kebanyakan kasus spam melibatkan program berbahaya dari keluarga Trojan perbankan yang mengambil data personal untuk mengakses layanan perbankan online. Temuan mencengangkan terjadi untuk perangkat dengan OS Android. Selama Juli lalu, SMS-Flooder.AndroidOS.Didat.a, yang menyasar sistem operasi Android, berada di posisi 15 dalam top 20 sehingga mencatat rekor baru untuk program di kategori ini. Fungsi yang dimiliki program ini memungkinkannya membuat dan mengirim pesan pendek secara massal.	Thomas (2013)
3	29/03/2016	Cheetah Mobile Security baru saja menemukan sebuah masalah. TrueCaller menggunakan IMEI ponsel sebagai cara untuk mengidentifikasi seseorang. Hal ini berarti, siapapun yang dapat melihat nomor IMEI dari aplikasi TrueCaller – baik melalui pencurian data atau cara lain – dan mencari nomor tersebut di situs TrueCaller dapat melihat informasi pribadi sang pemilik ponsel. Informasi tersebut diantaranya nama, jenis kelamin, alamat email, alamat rumah dan informasi lain yang TrueCaller simpan. *Hacker* juga dapat memodifikasi akun sang korban, menghilangkan blokir nomor spam dan	David (2016)

		membuat nomor spam tersebut dapat kembali masuk.	
4	11/07/2016	Game yang memanfaatkan teknologi AR (*Augmented Reality*) ini akan meminta para pemainnya untuk berjalan di dunia nyata untuk mencari Pokemon, Pokestop atau Gym. Pemain juga dapat menggunakan benda-benda tertentu atau item, yang ditemukan dalam game atau dibeli dengan uang asli, untuk menarik Pokemon di Pokestop. Kepolisian O'Fallon menyebutkan, hal inilah yang dimanfaatkan oleh para perampok. Selain perampok, popularitas Pokémon GO juga menarik perhatian para kriminal dunia cyber. Mereka menanamkan *malware* pada aplikasi Pokémon GO. Hal ini menjadi berbahaya karena Pokémon GO baru diluncurkan secara resmi di beberapa negara saja. Jadi, orang-orang yang tidak sabar menunggu rilisan resmi dari game ini akan mengunduh Pokémon GO dari situs yang tidak resmi.	Fatimah (2016)

Banyak faktor-faktor apa menyebabkan kasus-kasus ini terjadi. Salah satu faktor yang diasumsikan menjadi pemicu diantaranya adalah rendahnya tingkat kesadaran pengguna internet terhadap aturan dalam berkomunikasi dengan menggunakan *smartphone*. Menurut Chin (2012) yang meneliti mengenai

keamanan dan privasi para pengguna *smartphone*. Pengguna harus memahami tantangan dan kekhawatiran bahwa saat ini harus mengoperasikan secara sensitif pada *smartphone* mereka dengan mengidentifikasi peluang terjadinya kebocoran informasi pribadi untuk meningkatkan keamanan perangkat yang digunakan pengguna. Hal di atas yang melandasi penulis dalam melakukan penelitian mengenai *security awareness* pada pengguna *smartphone* secara lebih khusus, yaitu pada sistem operasi Android yang memiliki karakteristik yang berbeda dengan sistem operasi lainnya seperti yang telah dipaparkan sebelumya

Hal di atas yang melandasi penulis dalam melakukan penelitian mengenai keamanan informasi dan privasi pada pengguna *smarthphone* lebih khususnya, yaitu pada smartphone dengan sistem operasi Android yang akan diukur dengan kategori *awareness*.

1.3 Perumusan Masalah

Menurut Al-Sehri Y (2012) Beberapa 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. Pengguna ponsel sering menyimpan informasi pribadi dan keuangan mereka di telepon mereka. Hal itu membuat mereka menjadi target malware dan phishing oleh para pelaku. Teori ini memaparkan bahwa *smartphone* yang sangat dikenal khususnya Android merupakan sistem operasi *mobile phone* yang memiliki resiko yang besar, dan dari kasus-kasus yang dipaparkan di latar belakang, masih banyak pengguna *smartphone* yang belum menyadari aturan keamanan dan privasi yang harus diperhatikan dalam menggunakan *smartphone.* Padahal, banyak kasus-kasus terjadi seputar dampak negatif karena kurangnya kesadaran kemanan dalam menggunakan *smartphone*, termasuk di Indonesia, diakibatkan oleh faktor ketidakpahaman akan keamanan informasi ketika, mendapatkan SMS/email dari orang tidak dikenal yang menyertakan link palsu yang merupakan website buatan penyerang untuk membuat *smartphone* terkena serangan malware yang mengakibatkan pengambilan data secara illegal sampai rusaknya internal dari

perangkat (*smartphone*) yang digunakan. Menurut Xu (2011) 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 yang menonjol yang berbeda dari isu-isu privasi *online* dibahas dalam studi sebelumnya. Informasi Privasi menjadi kekhawatiran pengguna tentang kemungkinan kehilangan privasi sebagai akibat dari pengungkapan informasi kepada pihak ketiga seperti pengembang aplikasi. penulis tertarik untuk melihat bagaimana kesadaran (*awareness*) pengguna *smartphone* Android dalam menggunakan media (*smartphone*) tersebut dengan penelitian yang berjudul **Pengukuran Kesadaran Keamanan Informasi dan Privasi pada Pengguna Smartphone Android di Indonesia**

1.4 Pertanyaan Penelitian

Rumusan masalah yang ingin diselesaikan dalam penelitian ini adalah :

1. Bagaimana *security awareness* pengguna *Smartphone* Android di Indonesia berdasarkan kelompok *Attittude* dan apakah terdapat hubungan dari keduanya?
2. Bagaimana *security awareness* pengguna *Smartphone* Android di Indonesia berdasarkan kelompok *Knwoledge* dan apakah terdapat hubungan dari keduanya?
3. Bagaimana *security awareness* pengguna *Smartphone* Android di Indonesia berdasarkan kelompok *Behaviour* dan apakah terdapat hubungan dari keduanya?
4. Bagaimana *privacy awareness* pengguna *Smartphone* Android di Indonesia berdasarkan kelompok *Attitude* dan apakah terdapat hubungan dari keduanya?

5. Bagaimana *privacy awareness* pengguna *Smartphone* Android di Indonesia berdasarkan kelompok *Knowledge* dan apakah terdapat hubungan dari keduanya?
6. Bagaimana *privacy awareness* pengguna *Smartphone* Android di Indonesia berdasarkan kelompok *Behaviour* dan apakah terdapat hubungan dari keduanya?

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan penelitian adalah memperoleh hasil kajian mengenai :

1. Untuk mengukur tingkat *Security Awareness* dari pengguna *Smartphone* Android di Indonesia berdasarkan *Attitude* dan melihat hubungan antara keduanya.
2. Untuk mengukur tingkat *Security Awareness* dari pengguna *Smartphone* Android di Indonesia berdasarkan *Knowledge* dan melihat hubungan antara keduanya.
3. Untuk mengukur tingkat *Security Awareness* dari pengguna *Smartphone* Android di Indonesia berdasarkan *Behaviour* dan melihat hubungan antara keduanya.
4. Untuk mengukur tingkat *Privacy Awareness* dari pengguna *Smartphone* Android di Indonesia berdasarkan *Attitude* dan melihat hubungan antara keduanya.
5. Untuk mengukur tingkat *Privacy Awareness* dari pengguna *Smartphone* Android di Indonesia berdasarkan *Knowledge* dan melihat hubungan antara keduanya.
6. Untuk mengukur tingkat *Privacy Awareness* dari pengguna *Smartphone* Android di Indonesia berdasarkan *Behaviour* dan melihat hubungan antara keduanya.

1.6 Manfaat Penelitian

1.6.1 Manfaat Teoritis

Penelitian ini memaparkan bagaimana sistem keamanan informasi pada *smartphone* Android dengan mengukur *information security* dan *privacy awareness* dari penggunanya. Hasil penelitian ini diharapkan memberikan pengetahuan berupa informasi, khususnya terkait dengan *information security* dan *privacy awareness* yang ada pada pengguna *smartphone* Android. Disamping itu, untuk menambah kesahihan 3 kategori *awareness* sebagai alat ukur dalam pengukuran *information security* dan *information privacy* terhadap pengguna *smartphone* Android, dan diharapkan dapat dijadikan sebagai rujukan penelitian berikutnya.

1.6.2 Manfaat Praktis

Hasil dari penelitian pengukuran *information security awareness* dan *privacy awareness* ini akan memiliki nilai yang baik dalam memberi pengetahuan serta masukan bagi para pengguna *smartphone* Android di Indonesia. Pengguna *smartphone* Android telah mencapai 1,8M diseluruh dunia, menurut dat*a www.statista.com* per desember 2015, maka dari itu hal ini adalah potensi besar dalam terjadinya resiko yang dialami oleh penggunanya dilihat dari banyaknya kasus pelanggaran keamanan dan privasi pada pengguna *smartphone* Android. Selain manfaatnya bagi pengguna *smartphone* Android, penelitian ini pula diharapkan secara praktis bagi para pengguna *smartphone* Android agar lebih waspada dalam menggunakan fitur-fitur *smartphone* termasuk aplikasi dalam penyebaran informasi di dalamnya. Selain itu pula manfaat bagi para pengguna *smartphone* Android dalam hal *awareness* ini adalah dengan lebih menjaga data-data pengguna agar tidak disalahgunakan. Dengan mengetahui tingkat *awareness* dari konsumen atau pengguna dari *smartphone*. Pada developer aplikasi Androi juga dapat meningkatkan penjualan aplikasinya dengan melihat tingkat *awareness* pengguna *smartphone* Android di Indonesia.

1.7 Ruang Lingkup Penelitian

1.7.1 Variabel Penelitian

Penelitian ini menggunakan 3 variabel, yaitu :

1. *Awareness level,* dengan sub variabel sebagai berikut:
   - *Attitude*
   - *Knowledge*
   - *Behaviour*
2. *Information Security,* dengan sub variabel sebagai berikut:
   - *Trust in app repository*
   - *Misconception about application testing*
   - *Security and agreement message*
   - *Pireted application*
   - *Adoption of security control*
   - *Spam SMS*
   - *Report for Security Incident*
3. Information Privacy, dengan sub variabel sebagain berikut:
   - *Perceived Surveillance*
   - *Perceived Intrusion*
   - *Secondary Use Information*

1.7.2 Lokasi dan Objek Penelitian

Lokasi dan Objek Penelitian yang peneliti gunakan yaitu :

a) Penelitian ini dilaksanakan di Indonesia.
b) Objek dari penelitian ini adalah pengguna *smartphone*

1.7.3 Waktu dan Periode Penelitian

Secara Keseluruhan penelitian ini akan dilaksanakan dalam waktu 5 bulan terhitung sejak bulan Oktober 2016 hingga Maret 2017. Penelitian ini terbagi dalam beberapa periode yaitu survei pendahulua, usulan penelititan, kegiatan lapangan seperti pembagian kuesioner kepada responden, pengolahan dan analisis data, hingga penyelesaian penelitian.

1.8 Sistematika Penelitian

BAB I PENDAHULUAN

Dalam bagian ini dijelaskan gambaran umum, perumusan masalah, pertanyaan penelitian, tujuan penelitian, manfaat penelitian, dan sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Dalam bagian ini akan dibahas tinjauan pustaka terkait dengan permasalahan dan variabel yang ingin ditelaah secara lebih mendalam, yaitu mengenai *information security amd privacy awareness* untuk kemudian digunakan dalam menyusun kerangka pemikiran dalam penelitian ini.

BAB III METODE PENELITIAN

Dalam bagian ini dijelaskan mengenai metode penelitian yang digunakan, meliputi jenis penelitian, variabel operasional, tahapan penelitian, teknik *sampling*, teknik pengumpulan data, pengujian reliabilitas, dan teknik analisis data.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Hasil penelitian dan pembahasannya diuraikan secara kronologis dan sistematis sesuai dengan perumusan masalah serta tujuan penelitian. Setiap aspek pembahasan dimulai dari hasil analisis data, kemudian diiterpretasikan dan selanjutnya diikuti oleh penarikan kesimpulan. Dalam kesimpulan juga dibandingkan dengan penelitian-penelitian sebelumnya atau landasan teoritis yang relevan.

BAB V KESIMPULAN DAN SARAN

Dalam bagian ini terdiri dari kesimpulan hasil penelitian dengan cara uraian padat dan saran yang merupakan implikasi kesimpulan dan berhubungan dengan masalah dan alternatif pemecahan masalah.