CYBER RISK CALCULATOR: APLIKASI MUDAH ALIH PENILAIAN RISIKO KESELAMATAN SIBER

AMIRA NATASHA ROSLAN
ZALINDA OTHMAN

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Berdasarkan data yang diperoleh dari portal rasmi Kementerian Komunikasi Dan Multimedia Malaysia, terdapat 90 peratus peningkatan kes jenayah siber yang telah dilaporkan pada tahun 2020 berbanding dengan tahun sebelumnya. Terutamanya dalam tempoh pelaksanaan Perintah Kawalan Pergerakkan, ramai masyarakat malaysia dari pelbagai peringkat umur perlu menggunakan internet untuk belajar, bekerja dan berhubung. Namum, ramai yang masih tidak peka atau ambil peduli tentang risiko jenayah siber dan cara selamat melayari internet, menyebabkan peningkatan tersebut. CyberRisk Calculator adalah sebuah aplikasi mudah alih untuk masyarakat Malaysia mengetahui tentang tahap risiko keselamatan siber mereka (Individu) dengan menjawab soalan tentang pendedahan risiko siber dan ianya akan dinilai dengan menggunakan 3 tahap risiko iaitu tinggi, sederhana dan rendah. Aplikasi ini juga mempunyai bahan bacaan dan infografik tentang pelbagai jenis kesedaran keselamatan siber. Ini adalah salah satu langkah interaktif untuk menambah pengetahuan pengguna tentang keselamatan siber dan membantu pengguna untuk lebih berwaspada semasa melayari internet. Cyber Risk Calculator juga mempunyai fungsi dimana pengguna boleh mendapatkan no telefon dan laman web untuk badan organisasi yang bertanggung jawab jika berlaku sebarang kecemasan ataupun kes berkenaan jenayah siber. Secara ringkasnya aplikasi Cyber Risk Calculator ialah sebuah aplikasi untuk menilai tahap risiko keselamatan siber dan memberi kesedaran tentang keselamatan siber kepada pengguna. Cyber Risk Calculator akan dibangun menggunakan Android Studio dan menggunakan Java sebagai bahasa pengaturcaraan

1 PENGENALAN

Pada abad ini, jenayah siber adalah jenis jenayah komputer yang baharu. Penipuan, pemusnahan atau pengubahan program atau data komputer, kecurian maklumat, penggodaman dan lain-lain bentuk jenayah siber termasuk dalam kategori jenayah ini. Perkembangan Internet sebagai alat komunikasi terkini dijangka menyediakan platform untuk pemindahan maklumat, seterusnya meningkatkan pengetahuan dan maklumat. Beribu-ribu laman web telah diaktifkan kerana tiada siapa yang boleh mengawal aliran maklumat dalam dunia atas talian. Internet menyebarkan semua jenis maklumat, sama ada benar dan tidak tepat, serta idea, falsafah, propaganda, dan, tentu saja, pornografi. Berdasarkan data yang diperoleh dari portal rasmi Kementerian Komunikasi Dan Multimedia Malaysia, terdapat 90 peratus peningkatan kes jenayah siber yang telah dilaporkan pada tahun 2020 berbanding dengan tahun sebelumnya. Terutamanya dalam tempoh pelaksanaan Perintah Kawalan Pergerakkan, ramai masyarakat malaysia dari pelbagai peringkat umur perlu menggunakan internet untuk belajar, bekerja dan berhubung. Namum, ramai yang masih tidak peka atau ambil peduli tentang risiko jenayah

siber dan cara selamat melayari internet, menyebabkan peningkatan tersebut. Oleh yang demikian, berlakulah peningkatan kes jenayah siber dalam kalangan masyarakat.

2 PENYATAAN MASALAH

Pandemik Covid-19 telah mencipta cabaran baharu kepada rakyat Malaysia apabila mereka perlu menyesuaikan diri dengan situasi "normal baharu" iaitu bekerja dari rumah dan pembelajaran jarak jauh dalam talian. Syarikat dan sekolah sedang mempercepatkan transformasi digital mereka bagi meneruskan kelangsungan hidup, dan menyebabkan keselamatan siber kini menjadi kebimbangan utama. Pertama sekali, ramai rakyat Malaysia tidak menyedari dan mengetahui tentang tahap risiko keselamatan siber masing-masing. Hal ini menyebabkan mereka merasakan mereka akan sentiasa selamat daripada jenayah siber dan melakukan perkara yang akan meningkatkan keterdedahan terhadap jenayah siber tanpa mereka sedar. Kedua, kebanyakan rakyat Malaysia tidak mempunyai kesedaran asas tentang keselamatan siber dan tidak tahu cara untuk kekal selamat dalam talian. Ahli Lembaga Pengarah CyberSecurity Malaysia (CSM) Jen (B) Tan Sri Mohd Azumi Mohamed berkata, "Masih ramai pengguna internet di Malaysia tidak cakna, naif dan bersikap tidak peduli mengenai kepentingan keselamatan siber sehingga terpedaya dan seterusnya menjadi mangsa jenayah siber", dipetik dari laporan Astro Awani. Akhir sekali, terdapat banyak mangsa jenayah siber yang tidak tahu organisasi mana yang harus dihubungi untuk melaporkan kes jenayah siber atau meminta bantuan. Pihak CyberSecurity Malaysia percaya bahawa terdapat banyak lagi kes yang mungkin tidak dilaporkan atau tidak disedari oleh mangsa dan perkara ini amatlah membimbangkan.

3 OBJEKTIF KAJIAN

Objektif utama bagi projek ini adalah untuk membangunkan sebuah aplikasi mudah alih yang berfungsi untuk mengira tahap risiko keselamatan siber pengguna. Selain itu, objektif projek ini juga adalah untuk membangunkan aplikasi yang dapat membantu pengguna memahami dan menambah kesedaran keselamatan siber mereka. Untuk mencapai matlamat ini, Aplikasi yang akan dibangunkan perlu mempunyai fungsi seperti berikut: i. Memberi soalan pendedahan risiko keselamatan siber dan menilai tahap risiko keselamatan siber pengguna. ii. Memberi kesedaran tentang keselamatan siber dengan bahan bacaan dan infografik. iii. Menyediakan

link dan nombor telefon untuk setiap organisasi yang berkaitan dengan keselamatan siber di Malaysia.

4 METOD KAJIAN

Untuk pembangunan aplikasi ini, jenis model yang akan digunakan ialah metodologi Waterfall. Metodologi Waterfall ialah pendekatan pengurusan projek yang menekankan perkembangan linear dari awal hingga akhir pembangunan. Metodologi ini ialah proses pembangunan berurutan yang mengalir seperti air terjun melalui semua fasa projek (Keperluan analisis, reka bentuk, pembangunan, pengujian, perlaksanaan dan penyelenggaraan), dengan setiap fasa berakhir sepenuhnya sebelum fasa seterusnya bermula.

4.1 Fasa Analisis Keperluan

Peringkat pertama melibatkan pengetahuan dan keperluan aplikasi yang hendak dibangunkan. Kandungan yang akan dikenalpasti dan dianalisis termasuklah tujuan, fungsi utama dan kaedah membangunkan aplikasi. Selain itu, skop bagi projek ini juga akan dikenalpasti dan dianalisis supaya projek ini dapat dikhususkan dengan baik.

4.2 Fasa Reka Bentuk

Pada fasa ini, reka bentuk antara muka aplikasi Cyber Risk Calculator akan dibentuk. Seterusnya, cara pengiraan tahap keselamatan siber, jenis soalan dan bahan pembelajaran akan dikenalpasti dan dikumpulkan. Dalam fasa ini, semua keperluan yang telah diperoleh dari fasa satu akan diproses dan akan menjadi satu bentuk penyelesaian. Reka bentuk perlu dilaksanakan dengan teliti untuk mencapai objektif utama pembangunan projek ini.

4.3 Fasa Pembangunan

Dalam fasa ini, pembangunan aplikasi Cyber Risk Calculator akan bermula. Aplikasi ini akan dibangunkan menggunakan perisian Android Studio dan Java akan digunakan sebagai Bahasa pengaturcaraan untuk aplikasi ini. Aplikasi ini dibangunkan mengikut pecahan modul, iaitu modul soalan untuk mengira tahap keselamatan siber pengguna, modul bahan bacaan dan modul pautan ke organisasi keselamatan siber Malaysia bagi mendapatkan bantuan berkenaan masalah siber. Pembahagian modul ini dilakukan supaya dapat memudahkan proses pembangunan aplikasi ini.

4.4 Fasa Pengujian

Pada fasa ini, aplikasi yang sudah siap dibangunkan akan diuji dengan teliti. Fasa ini amat penting untuk memastikan sama ada semua objektif aplikasi ini telah dicapai dan dapat berfungsi dengan baik. Pada masa yang sama, kesilapan ataupun ralat dalam aplikasi juga dapat dikenalpasti. Hal ini sangat penting supaya pengguna dapat menggunakan aplikasi ini dengan baik dan tidak menghadapi sebarang masalah.

4.5 Fasa Perlaksanaan

Apabila aplikasi dapat berfungsi dengan baik dan tiada lagi masalah, aplikasi Cyber Risk Calculator akan didaftarkan ke Gedung aplikasi (Play Store) dan ia akan disebarkan kepada pengguna untuk diuji. Pengguna akan menggunakan aplikasi dan memberi maklum balas tentang pengalaman menggunakan aplikasi ini dari segi fungsi, kesesuaian reka bentuk dan adakah aplikasi ini telah mencapai objektif dan keperluan pengguna.

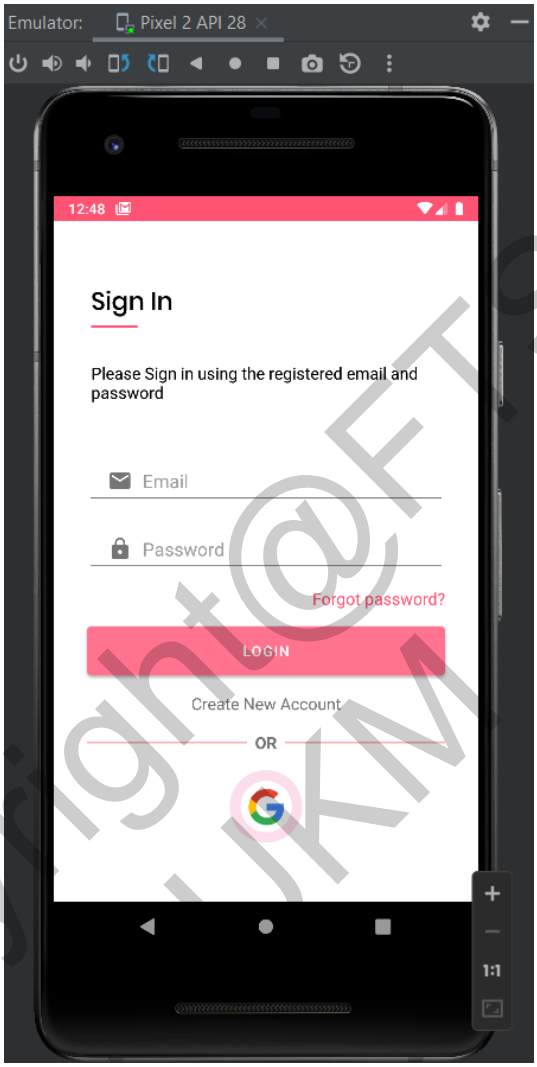
4.6 Fasa Penyelenggaraan

Fasa ini diperlukan jika terdapat sebarang penambahbaikan terhadap aplikasi ataupun jika masih ada kesilapan yang harus dibaiki. Fasa ini juga digunakan sekiranya terdapat permintaan dari pengguna untuk membuat perubahan atau penambahbaikkan pada reka bentuk mahupun isi kandungan aplikasi supaya pengguna dapat pengalaman maksimum menggunakan aplikasi ini.

5 HASIL KAJIAN

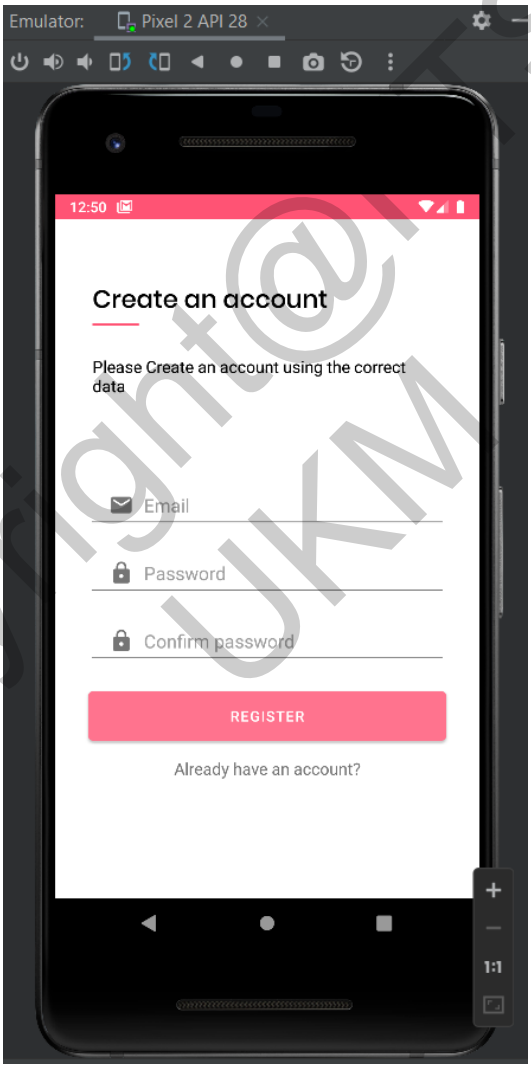
Aplikasi Cyber Risk Calculator dicipta dengan Android Studio, yang merupakan Integrated Development Environment (IDE) untuk membangunkan aplikasi Android. Firebase telah dipilih sebagai pangkalan data utama untuk aplikasi Cyber Risk Calculator semasa pembangunan. Perisian ini terdiri daripada antara muka yang membolehkan pengguna menjawab soalan risiko keselamatan siber, membaca nota kesedaran siber dan 61 mendapatkan bantuan siber.

Paparan utama program yang pengguna lihat ialah antara muka log masuk. Pengguna mesti memasukkan e-mel dan kata laluan berdaftar mereka. Antara muka log masuk pengguna dipaparkan seperti Rajah 1.



Rajah 1 Antara muka log masuk

Pengguna yang masih belum mendaftar e-mel dan kata laluan mereka mesti berbuat demikian agar maklumat mereka disimpan dalam pangkalan data aplikasi dan membolehkan mereka log masuk. Antara muka pendaftaran pengguna untuk Aplikasi Cyber Risk Calculator ditunjukkan dalam Rajah 2.



Rajah 2 Antara muka daftar pengguna

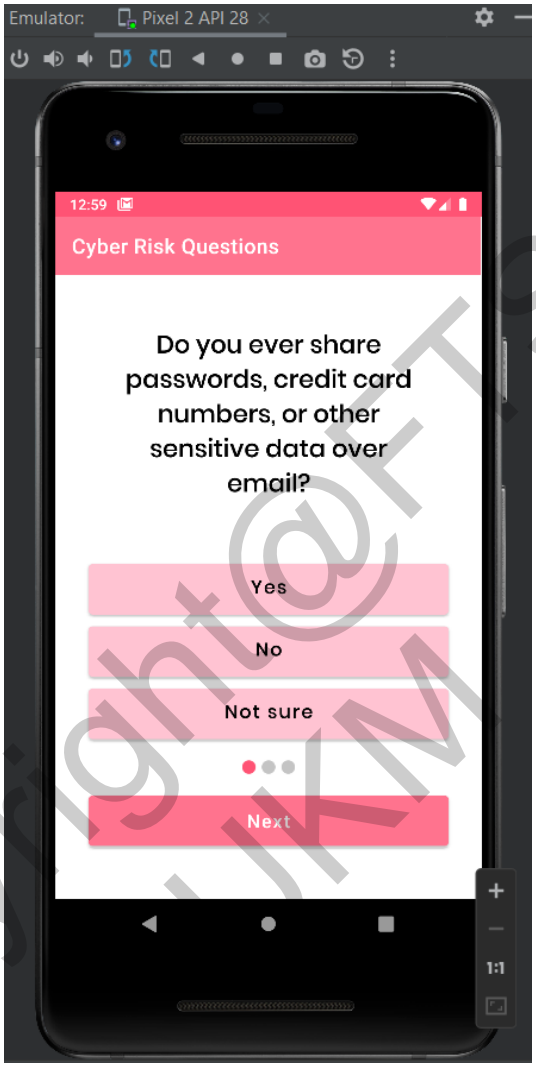
Skrin halaman utama akan muncul setelah pengguna mendaftarkan e-mel dan kata laluan atau log masuk ke dalam aplikasi. Rajah 4 menunjukkan antara muka laman utama untuk aplikasi Cyber Risk Calculator.

Rajah 4 Antara muka halaman utama

Halaman antara muka profil pengguna akan memaparkan maklumat pengguna seperti yang telah didaftarkan. Pengguna boleh mengubahsuai maklumat mereka dengan menyentuh ikon. Rajah 5 menunjukkan antara muka profil pengguna bagi aplikasi ini.

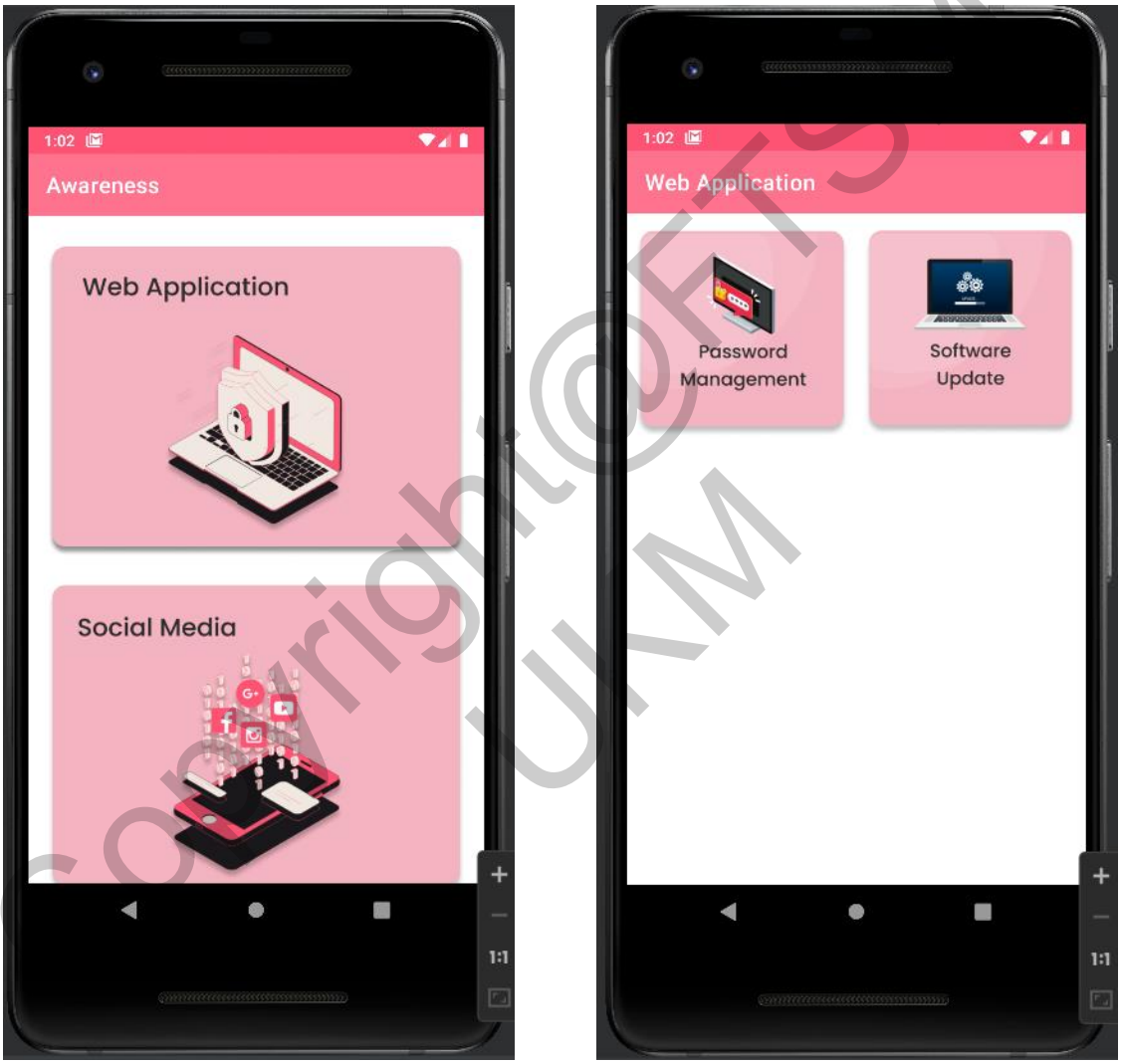
Rajah 5 Antara muka profil pengguna

Pada halaman ini, pengguna perlu menjawab kesemua 15 soalan risiko keselamatan siber untuk mengetahui tahap risiko keselamatan siber mereka. Rajah 6 menunjukkan antara muka soalan risiko keselamatan siber.



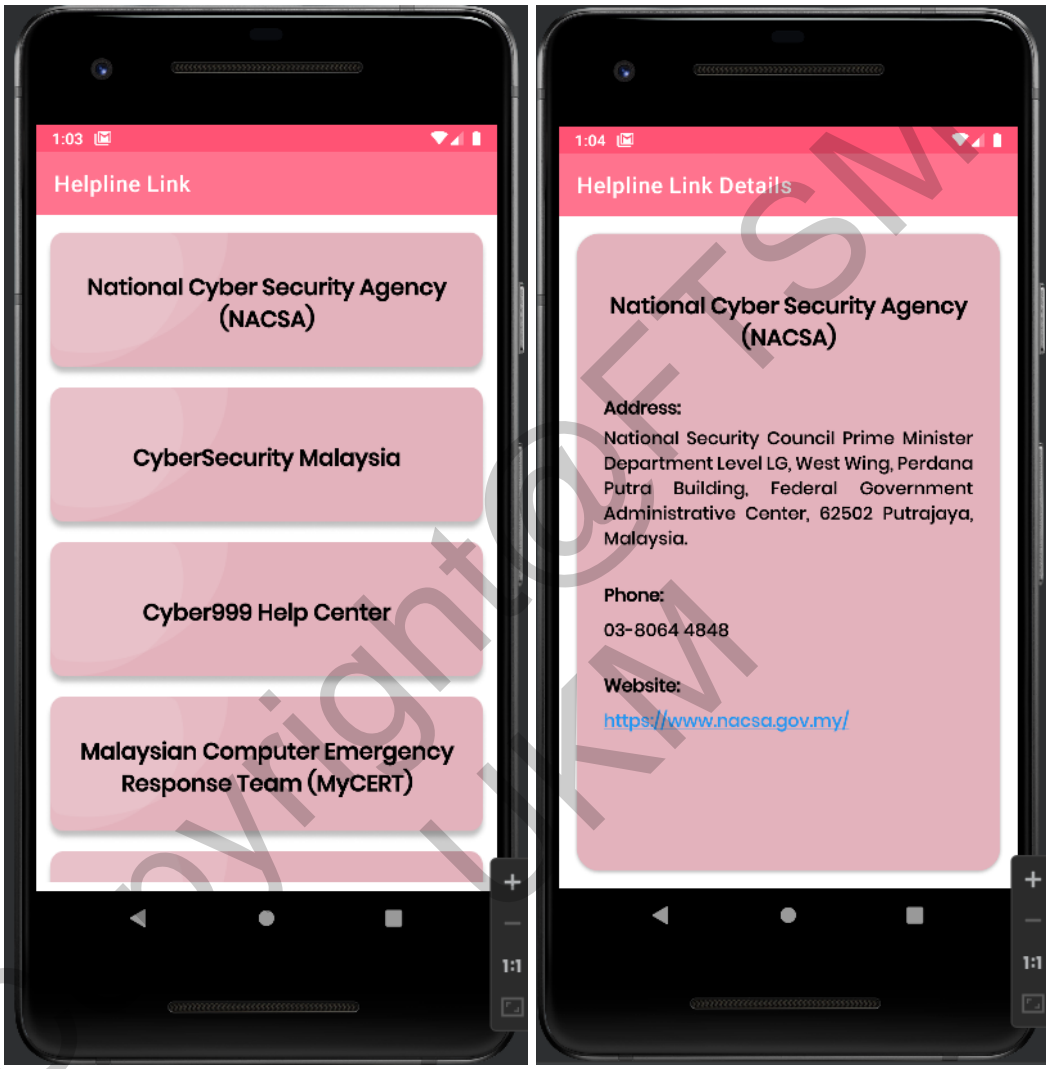
Rajah 6 Antara muka soalan risiko keselamatan siber

Melalui antara muka nota kesedaran keselamatan siber ini, pengguna dapat membaca bahan bacaan tentang topik keselamatan siber. Paparan antaran muka nota kesedaran keselamatan siber ditunjukkan dalam rajah 7.



Rajah 7 Antara muka nota kesedaran keselamatan siber

Pada paparan ini, pengguna dapat mengambil maklumat tentang agensi keselamatan yang ada di Malaysia. Rajah 8 menunjukkan antara muka pautan bantuan agensi keselamatan.



Rajah 8 Antara muka pautan bantuan agensi keselamatan

6 KESIMPULAN

Kesimpulannya, keseluruhan pembangunan aplikasi Cyber Risk Calculator ini berjaya mencapai objektif kajian iaitu untuk membangunkan aplikasi yang boleh mengira tahap keselamatan siber pengguna dan juga memberi nota atau inforgrafik tentang kesedaran keselamatan siber. Aplikasi ini juga berjaya menarik perhatian pengguna untuk mempelajari dan menambah ilmu kesedaran keselamatan siber mereka.

7 RUJUKAN

Astroawani.com. 2021. Ramai pengguna internet tidak peduli kepentingan keselamatan siber – Cybersecurity Malaysia. https://www.astroawani.com/beritahttps://www.astroawani.com/beritamalaysia/ramai-pengguna-internet-tidak-peduli-kepentingan-keselamatan-sibercybersecurity-malaysia-295878malaysia/ramai-pengguna-internet-tidak-pedulikepentingan-keselamatan-siberhttps://www.astroawani.com/berita-malaysia/ramaipengguna-internet-tidak-peduli-kepentingan-keselamatan-siber-cybersecuritymalaysia-295878cybersecurity-malaysia-295878 [28 Oktober 2021].

CyberSecurity Malaysia. (2013). ISMS Implementation Guideline A Practical Approach. https://www.cybersecurity.my/data/content_files/11/1170.pdf?.diff=1375349394 [14 April 2022].

Stoneburner, G., Goguen, A. and Feringa, A., 2002. Risk management guide for information technology systems. Gaithersburg: U.S. Dept. of Commerce, National Institute of Standards and Technology.

Law, L., 2021. Special Cyber Court and E-Court – Lee & Poh Partnership. https://lpplaw.my/special-cyber-court-and-e-court/ [27 Oktober 2021].

Amira Natasha Roslan (A182774)
Zalinda Othman
Fakulti Teknologi & Sains Maklumat,
Universiti Kebangsaan Malaysia