



UNIVERSITI PUTRA MALAYSIA

**KESEDARAN DAN AMALAN KESELAMATAN KOMPUTER
DAN INTERNET DI KALANGAN PEGAWAI DAN PENOLONG
PEGAWAI SISTEM MAKLUMAT DI LIMA KEMENTERIAN
PERSEKUTUAN DI MALAYSIA**

CHING THOO A/L KIM

FBMK 2002 20

**KESEDARAN DAN AMALAN KESELAMATAN KOMPUTER
DAN INTERNET DI KALANGAN PEGAWAI DAN PENOLONG PEGAWAI
SISTEM MAKLUMAT DI LIMA KEMENTERIAN
PERSEKUTUAN DI MALAYSIA**

Oleh

CHING THOO A/L KIM

**Tesis ini Dikemukakan Kepada Sekolah Pengajian Siswazah, Universiti Putra
Malaysia, Sebagai Memenuhi Keperluan untuk Ijazah Master Sains**

November 2002



Abstrak tesis yang dikenakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Ijazah Master Sains

**KESEDARAN DAN AMALAN KESELAMATAN KOMPUTER DAN
INTERNET DI KALANGAN PEGAWAI DAN PENOLONG PEGAWAI
SISTEM MAKLUMAT DI LIMA KEMENTERIAN
PERSEKUTUAN DI MALAYSIA**

Oleh

CHING THOO A/L KIM

November 2002

Pengerusi : Prof. Madya Dr. Musa Abu Hassan, Ph.D.

Fakulti : Bahasa Moden dan Komunikasi

Penggunaan teknologi komunikasi di organisasi awam meningkat dari sehari ke sehari. Tidak dinafikan penggunaan komputer misalnya, telah meningkatkan produktiviti dan keberkesanan jabatan kerajaan. Walau bagaimanapun, isu pencerobohan ke atas laman web beberapa jabatan kerajaan menimbulkan dua persoalan; kesedaran keselamatan komputer/Internet di kalangan kakitangan sektor awam berada pada tahap rendah, dan langkah keselamatan komputer/Internet yang digunakan tidak efektif untuk menangani serangan berkenaan. Oleh yang demikian kajian ini dijalankan untuk melihat dua aspek, mengenal pasti tahap kesedaran keselamatan komputer/Internet di kalangan kakitangan organisasi awam pada persepsi Pegawai Sistem Maklumat dan Penolong Pegawai Sistem Maklumat, dan mengenal pasti amalan-amalan

keselamatan komputer/Internet yang diamalkan oleh kakitangan organisasi awam di Malaysia

Kajian ini menggunakan borang soal selidik untuk mendapatkan data daripada responden di lima kementerian. Data yang diperoleh seterusnya dianalisis dengan menggunakan perisian '*SPSS for Windows*' versi 10.0.

Hasil kajian secara umumnya mendapat kesedaran keselamatan komputer/Internet kakitangan organisasi awam pada persepsi responden berada pada tahap rendah. Majoriti responden juga mengatakan tahap keselamatan komputer/Internet organisasi awam juga berada pada tahap rendah.

Kajian ini juga mendapat virus merupakan ancaman utama kepada laman web organisasi awam. Penggunaan perisian anti virus dan '*firewall*' pula merupakan amalan keselamatan yang kerap digunakan. Secara umumnya pelaksanaan amalan keselamatan komputer/Internet di kalangan responden berada pada tahap tinggi. Kajian juga mendapat penggunaan teknologi keselamatan Internet terkini seperti teknologi enskripsi di organisasi awam juga memuaskan.

Oleh yang demikian, kakitangan organisasi awam perlu diberikan pendedahan bagi meningkatkan kesedaran keselamatan komputer/Internet mereka. Sehubungan dengan ini juga, aspek latihan juga boleh menambahkan pengetahuan kakitangan organisasi awam dalam usaha melengkapkan diri.

mereka untuk berdepan dengan isu keselamatan komputer/Internet di sektor awam.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in
fulfillment of the requirement for the degree of Master of Science

**COMPUTER AND INTERNET SECURITY AWARENESS AND PRACTISES
AMONG INFORMATION TECHNOLOGY OFFICERS AND ASSISTANT
OFFICERS AT FIVE FEDERAL MINISTRIES MALAYSIA**

By

CHING THOO A/L KIM

November 2002

Chairman : Assoc. Prof. Dr. Musa Abu Hassan, Ph.D.

Faculty : Modern Languages and Communication

The adoption of communication technology in Malaysian's public sector has increased tremendously. For instance, the using of computer brought better productivity in several agencies and departments. However, the attack on several department's websites brought about two issues that need urgent attention. First, it shows that the level of computer/Internet security awareness among members of public sector was low, and second, the measures taken to address the incidents were rather inadequate or ineffective. Hence, this study aims at, first, identifying the level of computer/Internet security awareness among government servants from respondent's perception. Secondly, to identify security measures or technologies used by the government servants to safeguard the ICT asset of the government.

Using questionnaire as the instrument, this study managed to attract 123 respondents from five ministries around the capital city. Data gathered were then analysed using SPSS For Windows (version 10.0) software.

Study revealed that the level of computer/Internet security awareness among government servants was low as perceived by the respondents. This statement was supported by the fact that the level of computer/Internet security in public sector in general was also low.

Study also shows that majority public organizations suffered virus attack to their websites. Hence, the most common security measures used were anti-virus software and firewall. It is also noted that the uses of the most advanced security technology such as encryption began to create impact in the public organization.

As such, to equip government servants with the necessary knowledge, they have to be exposed to various training, courses, and seminar. Another important aspect was training. Through training, government servants will gain valuable knowledge, which can be used to deal with the computer/Internet security in the public sector.

PENGHARGAAN

Setinggi-tinggi ucapan terima kasih kepada organisasi dan individu-individu berikut:

Kerajaan Malaysia dan Jabatan Perkhidmatan Awam Malaysia kerana menaja pengajuan penulis di UPM.

Penyelia dan Jawatankuasa Penyeliaan Tesis di atas buah fikiran, nasihat dan dorongan yang dihuluskan.

Kementerian Penerangan Malaysia, MAMPU, dan MIMOS Berhad di atas kerjasama yang diberikan.

123 responden yang menjayakan kajian ini.

Kedua-dua ibubapa yang sentiasa mendoakan kejayaan penulis.

Dwen, Di Di dan Ci Ci di atas pengorbanan dan sokongan yang dicurahkan.

Sekian, terima kasih.

SENARAI KANDUNGAN

Muka Surat

ABSTRAK	ii
ABSTRACT	v
PENGHARGAAN	vii
LEMBARAN PENGESAHAN	viii
PERNYATAAN KEASLIAN	x
SENARAI KANDUNGAN	xi
SENARAI JADUAL	xiv
SENARAI RAJAH	xvi

BAB

I PENDAHULUAN	
Latar Belakang Kajian	1
Sejarah Internet Sepintas Lalu	4
Sejarah Internet Di Malaysia	5
Kenyataan Masalah	6
Objektif Kajian	10
Kepentingan Kajian	11
Skop Kajian	13
Limitasi Kajian	14
II KAJIAN BAHAN BERTULIS	
Pendahuluan	15
Definisi Keselamatan	16
Malaysia Memasuki Era ICT	20
Senario Penggunaan Internet Di Malaysia	28
Senario Penggunaan Internet Di Peringkat Global	31
Bentuk Ancaman Keselamatan Internet	32
Motif Serangan Ke Atas Internet	37
Rangka Dasar Keselamatan ICT Kerajaan	38
Mekanisme Pelaporan Insiden Keselamatan ICT	45
Buku Panduan Pengurusan Keselamatan ICT	
Sektor Awam Malaysia (MyMis)	48
Kajian Lampau Mengenai Keselamatan Internet	48
Amalan Keselamatan Internet	60
Tujuan Penggunaan Internet	64
Teori Penerimaan Teknologi	68
Pembentukan Rangka Konsep	71

III	METODOLOGI KAJIAN	
Pendahuluan	73	
Lokasi Kajian	73	
Populasi Dan Pensampelan	74	
Unit Analisis	80	
Reka Bentuk Kajian	80	
Instrumen Kajian	82	
Pengukuran Angkubah Kajian	84	
Pra Uji	90	
Pengumpulan Data	92	
Penganalisisan Data	93	
IV	HASIL KAJIAN DAN PERBINCANGAN	
Pendahuluan	94	
Ciri Demografi Responden	94	
Tahap Penggunaan Aplikasi Komputer	97	
Tahap Penggunaan Internet	99	
Tujuan Penggunaan Komputer	101	
Tujuan Penggunaan Internet	101	
Kekerapan Penggunaan Komputer dan Internet	104	
Kesedaran Keselamatan Komputer/Internet Di Kalangan Kaki tangan Organisasi Awam	106	
Tahap Kesedaran Keselamatan Komputer/Internet Di Kalangan Kaki tangan Organisasi Awam		
Pada Persepsi Responden	106	
Amalan Keselamatan Komputer/Internet		
Di Organisasi Awam	108	
Jenis Amalan Keselamatan	108	
Kekerapan Pelaksanaan Amalan Keselamatan	109	
Tahap Pelaksanaan Amalan Keselamatan	110	
Latihan Berkaitan Keselamatan Komputer/Internet	113	
Latihan dan Tahap Pelaksanaan Amalan Keselamatan	115	
Bentuk Gangguan Ke Atas Laman Web		
Organisasi Awam	116	
Langkah-Langkah Yang Perlu Diambil Oleh Organisasi Awam Untuk Mengatasi Serangan Ke Atas Laman Web	117	
Cadangan Langkah Untuk Meningkatkan Tahap Kesedaran Keselamatan Komputer/Internet		
Kaki tangan Organisasi Awam	118	
Cadangan Bentuk Latihan Untuk Meningkatkan Pengetahuan Kaki tangan Organisasi Awam		
Terhadap Keselamatan Komputer/Internet	119	
Rumusan	121	

V	RINGKASAN, KESIMPULAN DAN CADANGAN	
	Ringkasan Kajian	122
	Kesimpulan	127
	Cadangan	129
	Cadangan Kajian Masa Hadapan	131
 BIBLIOGRAFI		
		133
 LAMPIRAN		
I	Pelanggan Internet Mengikut Negeri (2000)	141
II	Borang Soal Selidik	142
 BIODATA PENULIS		
		159

SENARAI JADUAL

Jadual		Muka Surat
1	Peruntukan Pembangunan Untuk Program Dan Projek Yang Berkaitan ICT, 2001-2005 (RM Juta)	23
2	Kadar Penetrası Internet di Malaysia	29
3	Statistik Penyalahgunaan Dalam Talian (On-line Abused)	55
4	Pecahan Populasi Kajian Mengikut Gred Jawatan	75
5	Pecahan Responden Kajian Mengikut Gred Jawatan	76
6	Pemilihan Sampel Kajian Mengikut Kementerian	77
7	Peratus Pemulangan Boiang Soal Selidik Mengikut Kementerian	78
8	Peratus Responden Mengikut Ciri-Ciri Demografi	96
9	Peratusan Tahap Penggunaan Aplikasi Komputer	97
10	Peratusan Keseluruhan Tahap Penggunaan Aplikasi Komputer	98
11	Ujian Khu Kuasa Dua Angkubah Kajian Terhadap Tahap Penggunaan Aplikasi Komputer Responden	99
12	Peratus Tahap Penggunaan Internet	100
13	Peratus Keseluruhan Tahap Penggunaan Internet	100
14	Peratusan Tujuan Penggunaan Komputer Dan Internet	102
15	Ujian Khi Kuasa Dua Di Antara Angkubah Bebas Dengan Tujuan Penggunaan Komputer Responden	103

16	Ujian Khı Kuasa Dua Di Antara Angkubah Bebas Dengan Tujuan Penggunaan Internet Responden	103
17	Peratus Kekerapan Tujuan Penggunaan Komputer Dan Internet	105
18	Peratusan Persepsi Responden Tahap Kesedaran Keselamatan Komputer/Internet Di Kalangan Kaki tangan Organisasi Awam	107
19	Peratus Kekerapan Amalan Keselamatan Komputer/Internet Di Organisası Awam	110
20	Peratusan Tahap Pelaksanaan Amalan Keselamatan Komputer/Internet	111
21	Tahap Pelaksanaan Amalan Keselamatan Komputer/ Internet Secara Keseluruhan	112
22	Ujian Khı Kuasa Dua Angkubah Kajian Terhadap Tahap Pelaksanaan Amalan Keselamatan Komputer/Internet	112
23	Peratusan Latihan Berkaitan Keselamatan Komputer/Internet	114
24	Ujian Khı Kuasa Dua Di Antara Latihan Dengan Tahap Pelaksanaan Amalan Kesedaran Keselamatan Komputer/Internet	115
25	Peratusan Bentuk Gangguan Ke Atas Laman Web Organisası Awam	116
26	Peratusan Langkah-Langkah Yang Perlu Diambil Untuk Mengatasi Serangan Ke Atas Laman Web Organisası Awam	118
27	Cadangan Langkah Untuk Meningkatkan Kesedaran Keselamatan Komputer/Internet Di Kalangan Kaki tangan Organisası Awam	119
28	Cadangan Bentuk Latihan Untuk Meningkatkan Tahap Pengetahuan Kaki tangan Organisası Awam Terhadap Keselamatan Komputer/Internet	120

SENARAI RAJAH

Rajah		Muka Surat
1	Jenis Ancaman Kepada Sistem Komputer	18
2	Model Penerimaan Teknologi	69
3	Rangka Konsep Kajian	72
4	Rangka Persampelan Kajian	79

BAB I

PENDAHULUAN

Latar Belakang Kajian

Kedatangan teknologi komunikasi dan maklumat (ICT) membawa cabaran baru kepada sesebuah negara dalam tiga aspek, iaitu sosio-politik dan budaya, ekonomi, dan keselamatan (Muhammad Rais Abd. Karim, 2001).

Cabaran sosio-politik dan budaya menyaksikan bagaimana sesebuah negara itu menangani isu dunia tanpa sempadan. Kepada kebanyakan negara sedang membangun dan mundur, terma seperti globalisasi, dunia siber dan sebagainya adalah asing bagi mereka. Mereka terpaksa berdepan dengan semua itu tanpa mempunyai '*management tools*' yang bersesuaian untuk menghadapinya. Rentetan daripada cabaran dan perubahan yang begitu drastik dalam ICT, terdapat negara yang tidak berupaya untuk mengikut arah aliran itu. Keadaan ini menyebabkan terdapat sesetengah negara kehilangan kawalan (*erosion of control*) terhadap hal-hal domestik negaranya. Sebagai akibatnya, negara tersebut hanya menjadi penerima kepada apa yang disogokkan oleh negara maju yang menyebabkan terhakisan nilai dan etika tempatan secara evolusi.

ICT juga membawa kepada 1untuhnya sempadan ekonomi sesebuah negara Kawalan negaia ke atas faktor-faktor ekonomi semakin berkurangan Sebaliknya entiti perniagaan mengambil alih peranan kerajaan dalam menentukan kek ekonomi sesebuah negara Keadaan ini membawa kepada pembahagian kekayaan dan pendapatan yang tidak seimbang di antara sekto1 masyarakat Sekiranya keadaan ini tidak dikawal, ia boleh mencetuskan masalah pe1kauman

Dalam pada itu, usaha untuk bergerak seiring dengan aius ICT menagih peruntukan yang besar Keadaan ini menyebabkan pembangunan sekto1-sekto1 lain diabaikan Kadang kala peruntukan yang besar ini tidak mendatangkan pulangan seperti yang diharapkan kerana pe1kaia asas seperti pembangunan tenaga manusia, pendidikan, kemudahan asas belum diatasi lagi Lantaran itu, juiang digital di antara '*haves*' dan '*haves not*' terus kekal dan malah semakin melebar (Muhammad Rais Abd Karim, 2001)

Isu keselamatan data dan maklumat yang disalurkan melalui rangkaian (Internet) adalah di antara faktor yang melambatkan penggunaan Internet untuk tujuan e-dagang di kalangan syarikat di Malaysia. Kajian yang dijalankan oleh 'Technowledge Asia' (1999) terhadap 3000 syarikat di Malaysia mendapati isu keselamatan data tersenarai di antara lima faktor utama yang melambatkan penggunaan Internet tujuan e-dagang di Malaysia. Faktor-faktor lain termasuklah kos, latihan, peralatan, dan isu privasi. Kajian mereka juga mendapati isu keselamatan juga tergolong di antara penyebab utama yang mempengaruhi pencapaian perniagaan syarikat-syarikat korporat di negara ini.

Walaupun langkah-langkah pencegahan telah diambil, masalah kelemahan pengawasan keselamatan ICT membatas usaha tersebut. Insiden-insiden keselamatan ICT seperti kecurian data dan maklumat kerajaan serta korporat, pencerobohan privasi individu, dan '*cyberattacks*' perlu ditangani terlebih dahulu bagi memastikan peluang yang dibawa oleh ICT dapat dimanfaatkan sepenuhnya.

Di Malaysia, kita digemparkan dengan berita serangan penggodam ke atas laman web rasmi Parlimen Malaysia dan beberapa agensi kerajaan lain seperti Jabatan Perkhidmatan Awam, Kementerian Kesenian, Kebudayaan dan Pelancongan dan sebagainya. Kejadian ini bukan sahaja menyebabkan kemusnahan kepada data dan maklumat kerajaan, malah mengurangkan keyakinan orang ramai terhadap yang perkhidmatan secara '*on-line*' yang

disediakan oleh kerajaan. Kejadian serangan ke atas laman web kerajaan mungkin boleh dielakkan sekiranya kakitangan yang dianamahkan menjaga sistem ICT kerajaan mempunyai tahap kesedaran yang tinggi mengenai keselamatan Internet di samping mempraktikkan amalan-amalan keselamatan Internet terkini di tempat kerja.

Sebelum kita dapat membuat sebarang kesimpulan mengenai tahap kesedaran dan amalan-amalan keselamatan Internet di kalangan kakitangan organisasi awam di Malaysia, satu kajian yang komprehensif perlulah diadakan terlebih dahulu. Oleh yang demikian, tujuan utama tesis ini adalah untuk mencari jawapan kepada kedua-dua persoalan tersebut. Adalah diharapkan hasil kajian kelak akan memberikan satu gambaran yang menyeluruh mengenai tahap kesedaran dan amalan keselamatan Internet di kalangan kakitangan organisasi awam di Malaysia.

Sejarah Internet Sepintas Lalu

Secara umumnya Internet bermula apabila Jabatan Pertahanan Amerika Syarikat membangunkan rangkaian komputer yang dikenali sebagai '*Advanced Research Projects Administration*' (ARPANET) pada tahun 1966 (Armbruster, 1994). ARPANET dipertanggungjawabkan untuk menjalankan penyelidikan teknologi tinggi (Ahmad Zaharin, 2000). Dari setahun ke setahun, semakin ramai organisasi di seluruh dunia dihubungkan ke ARPANET. Bagi mewakili komposisinya yang

semakin membesar, maka ARPANET telah mendapat nama baru iaitu Internet (Sellappan, 1997)

Sejarah Internet di Malaysia

Sejarah dan perkembangan media baru di Malaysia bermula dengan pembelian komputer oleh Lembaga Letuk Negera (sekarang dikenali sebagai Tenaga Nasional Berhad) pada tahun 1966. Sementara itu, perkhidmatan telefon pula bermula sejak tahun 1874 lagi. Ini diikuti dengan penubuhan Jabatan Telekomunikasi pada tahun 1946 (Musa, 2002).

Percubaan untuk membangunkan rangkaian komputer pertama di Malaysia sebenarnya bermula di bawah Rancangan Malaysia Kelima (1986-1990) lagi. Usaha berkenaan dipelopori oleh sekumpulan pensyarah dari Fakulti Kejuruteraan Universiti Malaya yang diketuai oleh Mohamed Awang-Lah. Usaha mereka telah membawa kepada kejayaan membangunkan rangkaian komputer pertama di Malaysia yang dikenali sebagai Rangkaian Komputer Malaysia atau RangKom pada tahun 1987 (Rahmah Hashim & Aifah Yusof, 1999, Ahmad Zaharin, 2000 & Musa, 2002).

Rakyat Malaysia buat pertama kali menikmati perkhidmatan Internet apabila Institut Sistem Mikroelektronik Malaysia atau Mimos melancarkan pembekal perkhidmatan Internet (ISP) yang dikenali sebagai 'Joint Advanced

Integrated Networking' (JARING) pada tahun 1992. Bertitik tolak dari situ, penggunaan Internet di Malaysia terus berkembang. Ini dapat dilihat dari kemunculan lima lagi 'ISP' iaitu Telekom Malaysia Berhad (TMnet), Maxis Broadband Sdn Bhd (Maxisnet), DiGi Telecommunication Berhad (Diginet), Celcom Berhad (Celcomnet), dan TimedotNet Berhad (Timedot.com) yang menawarkan perkhidmatan Internet kepada rakyat Malaysia (Gan & Stephen, 2001).

Kenyataan Masalah

Pertumbuhan paling pesat dunia Internet hari ini nampaknya datang dari pada penggunaan '*World Wide Web*' (WWW). Pada asalnya WWW dicipta untuk digunakan secara terbuka atau '*complete openness*'. Aspek keselamatan tidak dipentingkan pada ketika itu. Walau bagaimanapun, pada masa sekarang jelas bahawa keselamatan diperlukan untuk menghadkan akses kepada satu-satu laman, melindungi kerahsiaan maklumat yang disalurkan melalui dan sebagainya (Lipp & Hassler, 1996).

Malah para sarjana pada hari ini, di dalam membincangkan kelebihan dan peluang yang ditawarkan oleh Internet, turut memberikan fokus kepada isu keselamatan Internet yang tidak kurang pentingnya. Malah salah satu isu utama keselamatan ICT negara ialah tahap kesedaran yang masih rendah di kalangan pihak pengurusan dalaman sistem keselamatan ICT (Mohd Ridzwan, 2001).

Kejadian serangan ke atas laman web, rangkaian komputer atau pangkalan data oleh penggodam, ‘cracker’, atau virus membuktikan bahawa isu keselamatan Internet tidak boleh diambil ringan. Dari kes-kes yang tadi, tidak keterlaluan jika dibuat kesimpulan bahawa data, maklumat malah rahsia yang disimpan di dalam komputer adalah terdedah kepada bahan pencerobohan. Kejadian ini juga menampakkan bahawa tahap keselamatan Internet adalah rapuh. Serangan ke atas lama web misalnya, bukan sahaja mengakibatkan kerugian dalam bentuk wang tinggi, malah menimbulkan kesangsian di kalangan orang ramai terhadap keupayaan organisasi berkenaan menyimpan data dan maklumat peribadi mereka dengan selamat.

Kerajaan Malaysia memandang seius kejadian serangan penggodam ke atas beberapa laman web jabatan dan agensinya. Menurut laporan yang dikeluarkan oleh Jawatankuasa Kebangsaan Mengenai Teknologi Maklumat (2001), sebanyak 68 laman web jabatan dan agensi kerajaan telah diserang dalam tempoh Februari 1999 hingga April 2001. Ini jelas menunjukkan bahawa rendahnya kesedaran mengenai pentingnya data dan maklumat kerajaan dilindungi. Kesimpulan juga dapat dibuat bahawa langkah-langkah keselamatan dalam institusi-institusi berkenaan yang longgar dan lemah tidak dinafikan turut menyumbang kepada kejadian ini.

Kejadian serangan pengganas ke atas ‘World Trade Centre’ (WTC) di New York dan ‘Pentagon’ di Washington DC pada 11 September 2001 mendesak

beberapa syarikat gergasi ICT dunia memperketatkan sistem keselamatan ICT masing-masing (H Amir Khalid, 2001) Kesedaran untuk mengadakan keselamatan fizikal bagi menghadapi bencana berkenaan meningkat di kalangan syarikat-syarikat berkenaan terutamanya untuk meminimumkan kerugian kepada perniagaan mereka

Diatas kesedaran ini telah mendorong syarikat IBM Corporation mewujudkan '*Office of Global Security Solutions*' Bahagian ini akan memberikan tumpuan khusus kepada teknologi untuk keselamatan fizikal, mengadakan kawalan akses kepada lokasi dan sumber, serta ancaman dalam bentuk '*biohazard*' seperti virus anthrax Pejabat ini juga diperintanggungjawabkan untuk mengesan dan mengenal pasti risiko-risiko keselamatan yang bakal dihadapi IBM juga akan membelanjakan sebanyak USD7 bilion untuk membangunkan teknologi keselamatan ICTnya sendiri

Bagaimana pula dengan tahap kesedaran keselamatan komputer/Internet di organisasi awam di Malaysia pada masa ini? Adakah serangan terhadap laman web kerajaan menunjukkan rapuhnya tahap keselamatan komputer/Internet di organisasi awam? Justeru itu, kajian ini diharapkan dapat menjawab persoalan kajian seperti berikut

- | Apakah tahap penggunaan aplikasi komputer dan Internet responden?