

Penipuan SMS Yang Perlu Anda Tahu



Oleh : Irwan Dahnil & Salleh Esa



SMS Scam : Yang Perlu Anda Tahu

Hakcipta Terpelihara 2008 oleh AkademiSMS.com

Ebook ini ditulis dan disusun dari bacaan, rujukan dan kajian yang telah dilakukan. Ia bertujuan untuk memberikan pendedahan kepada semua pihak mengenai penyalahgunaan SMS yang boleh membawa kesan yang negatif.

Anda digalakkan untuk mengedarkan kepada semua kenalan anda, pelanggan, keluarga dan juga rakan anda bagi melindungi mereka dari terlibat dengan penipuan seperti yang dinyatakan.

Namun, anda dilarang untuk mengubah kandungan di dalam ebook ini tanpa kebenaran dan pengetahuan penulis. Untuk mengetahui usaha penulis layari www.akademisms.com

Rekabentuk ecover dan banner disumbangkan oleh designer Luvlee di www.cheapest-cover.com

<u>Isi Kandungan</u>	<u>Muka Surat</u>
Prakata	4
Pengenalan	5
Modus Operandi I - Penipuan Aktif	6
Modus Operandi II - Penipuan Pasif	7
Manipulasi Sistem SMS	
SMS Broadcast	
SMS Subscribe	
SMS IOD	
Menggunakan Sistem SMS Secara Hybrid	
Adakah Anda Prospek Menjadi Mangsa	16
Kaedah Penipuan SMS	17
Kes-kes Yang Melibatkan Penyedia Gateway	20
Beberapa Kes Yang Melibatkan Syarikat Ternama	24
Respon Syarikat Ternama Terhadap Penipuan SMS	27
Bagaimana Menangani SMS Scam	29
Panduan dan Ingatan Dari Telco	31
Perancangan Kerajaan Terhadap SMS Scam	34
Rujukan	35
Mengenai Penulis	36
Mengenai Akademisms.com	37

Prakata

Saban hari, isu sindiket penipuan SMS semakin meningkat. Ada yang menjanjikan habuan hadiah wang tunai yang lumayan, imbuhan yang menarik dan sukar untuk dilepaskan. Pelbagai cara untuk melakukan penipuan tersebut.

Tetapi mengapa ini berlaku ? Adakah sifat tamak pengguna yang ingin cepat kaya dan mengharap tuah yang datang bergolek ? Atau kerana pengguna yang tidak celik dengan kaedah penipuan zaman baru yang menggunakan internet dan SMS ?

Disebabkan itu pengguna tidak dapat membezakan antara perniagaan dan pemasaran SMS yang asli dengan scam dan penipuan SMS. Mungkin dari segi teknikalnya, pengguna tidak nampak bagaimana ia beroperasi menyebabkan ia agak sukar untuk dibezaan.

Ebook ini bertujuan untuk mendedahkan isu-isu hangat seperti ini bagi memberi pemahaman dan kesedaran kepada pengguna mengenai bentuk-bentuk penipuan SMS. Modus operandi dan kaedah penipuan yang biasa digunakan juga akan didedahkan supaya pengguna tidak terjebak lagi dengan kes-kes yang berulang.

Di akhir ebook ini juga diberikan beberapa langkah dan tips tentang apa yang perlu anda lakukan supaya anda tidak terpedaya. Bagi mereka yang pernah terjebak, apakah yang perlu lakukan dan apakah hak anda sebagai pengguna.

Semoga ebook ini dapat member manfaat kepada anda untuk menjadi pengguna yang bijak.

Salam Usahawan!

Irwan Dahnil & Salleh Esa

Pengenalan

Apa itu SMS

Secara mudah, SMS (Short Message Service) boleh ditakrifkan sebagai suatu perkhidmatan yang ditawarkan melalui telefon bimbit atau internet untuk mengirim atau menerima pesanan pendek.

Apa itu SCAM ?

SCAM ditakrifkan sebagai penipuan secara terancang dengan menyediakan pulangan yang lumayan sekiranya anda menyertai program, aktiviti atau skim yang SCAMMER tawarkan.

Pihak yang mengendalikan jenayah ini digelar sebagai SCAMMER. SCAMMER melakukan penipuan secara terancang dimana perkara-perkara seperti nama, alamat, logo, nombor telefon danwakil syarikat dipalsukan untuk mendorong pengguna mempercayainya.

Sebagai contoh, SCAMMER akan membuat pengakuan bahawa mereka adalah dari sebuah syarikat yang terkenal.

Ciri-ciri syarikat yang selalu ‘dijaja’ adalah syarikat yang mengendalikan program reality tv, syarikat GLC atau syarikat yang pernah menganjurkan pertandingan dan menawarkan ganjaran yang lumayan.

Sebagai contoh, pihak SCAMMER menamakan diri mereka sebagai Astro, Petronas, Celcom, Maxis, Hotlink, GangStarz, DiGi, Shell, Bank dan Akademi Fantasia.

SCAMMER juga bersiap sedia dengan kononya menyediakan khidmat perkhidmatan pelanggan untuk dihubungi bagi memudahkan pembaca SMS tersebut membuat rujukan dan panduan menyertai program yang dianjurkan.

Modus Operandi I – Penipuan Secara Aktif

Ia boleh dikategorikan kepada dua kaedah penipuan iaitu penipuan secara pasif atau penipuan secara pasif.

Untuk penipuan secara aktif, SCAMMER akan menyediakan unit khidmat pelanggan bagi menghubungi mangsa melalui telefon dan menerangkan secara terperinci kepada bakal mangsa mereka.

Antara kaedah yang biasa dilakukan adalah dengan mereka ini akan mendapatkan nombor telefon mangsa dan mengucapkan tahniah diatas kemenangan cabutan bertuah.

Mangsa pula akan diberikan masa yang singkat untuk berfikir dan membuat tindakan untuk menebus ganjaran yang ditawarkan. Dengan pendekatan psikologi, mereka membuatkan mangsa tidak mempunyai masa yang panjang untuk berfikir dan membuat keputusan segera. Dengan cara itu mereka boleh mendapatkan maklumat No. Kad Pengenalan, Alamat, Kad ATM dan Akaun Bank dan cara-cara pengaktifan akaun bank melalui internet sahaja.

Ia kelihatan seperti tidak logik, tetapi tindakan licik mereka ini dikaburi dengan kaedah untuk mendapatkan maklumat melalui pengesahan kemenangan atau maklumat-maklumat alamat terkini.

Contoh Maklumat Pengesahan Kemenangan:

“ Sila sahkan maklumat berikut ; nama penuh anda, no. kad pengenalan, no. kad atm, no. akaun bank dan alamat terkini. Maklumat ini akan memudahkan proses pembayaran dan mengelakkan sebarang kesilapan berlaku.”

Contoh Maklumat Pengesahan Alamat Terkini :

"Sila sahkan alamat terkini anda beserta nama penuh, no. kad pengenalan, no. kad atm dan no. akaun bank untuk mengelakkan sebarang kesilapan berlaku. "

Mangsa yang mudah terpedaya akan menghantar maklumat-maklumat peribadi mereka dengan segera kerana berpendapat bahawa beliau hanya perlu membala SATU SMS sahaja untuk mendapatkan ganjaran lumayan yang dijanjikan dalam tempoh beberapa minit sahaja lagi.

Atas dasar sifat inginkan hadiah atau ganjaran bernilai ribuan ringgit, mangsa terus membala SMS tersebut dengan segera tanpa perlu berfikir secara rasional.

Modul Operandi II - Penipuan Secara Pasif

Satu lagi pendekatan penipuan dilakukan adalah dengan cara pasif dimana ia tidak melibatkan unit khidmat pelanggan. Sebaliknya ia menggunakan sistem perkhidmatan SMS yang telah diaturcara dan beroperasi secara automatik.

Di pasaran sekarang, terdapat pelbagai aplikasi SMS yang boleh dibeli atau dilanggan. Sesetengah aplikasi tersebut boleh didapati secara percuma atau boleh dilanggan dengan kos yang rendah.

Sistem ini sekiranya digunakan secara tidak beretiika oleh SCAMMER boleh dimanipulasikan bagi tujuan menipu mangsa. Tiga aplikasi yang boleh dimanipulasikan untuk tujuan menipu adalah seperti SMS IOD, SMS Subscribe dan SMS Broadcast.

1. Manipulasi SMS Broadcast

SMS Broadcast adalah satu aplikasi berasaskan web yang membolehkan SCAMMER untuk menghantar SMS kepada satu atau banyak nombor telefon bimbit. Seperti email, hanya dengan satu klik,

SMS tersebut boleh dihantar kepada beribu-ribu nombor dengan cepat.



SMS Broadcast ini mempunyai keistimewaan yang apabila SCAMMER boleh menyembunyikan identity pengirim SMS dengan menggantikan dengan nama yang lain. Berbeza dengan penghantaran SMS biasa dari telefon bimbit ke telefon bimbit, dengan menggunakan SMS Broadcast SCAMMER menggantikan pengirim identity pengirim dengan memasukkan nama syarikat-syarikat besar seperti Maxis, SHELL, Petronas dan sebagainya untuk tujuan menipu pelanggan.

Oleh itu mangsa tidak dapat membezakan SMS yang telah diterima sama ada asli atau tidak.

Sender ID	Maxis	Note: Maxis number will appear "31000000" as sender id
Number To Multiple Numbers Line By Line: (Copy & Paste inside the box) * International format e.g: (Malaysia) 60191234567 60123333333 60167777777 60142223333 60132223334 60172223337 (maximum 1000 numbers at one time)	60191234567 60123333333 60167777777 60142223333 60132223334 60172223337	<p style="color: red;">Identiti Pengirim Boleh Diubah Digantikan Dengan Yang Lain contohnya Maxis</p> <p style="color: red;">Banyak Nombor Boleh Dihantar Secara Serentak</p>

Satu lagi kelebihan SMS Broadcast adalah kemampuan untuk menghantar SMS keluar negara. Maka tidak hairanlah sekiranya ada diantara mangsa yang menerima SMS dari nombor yang pelik dan bukannya kod telefon Malaysia.

Ini biasanya adalah sindiket penipuan yang dilakukan dari luar negara untuk menipu mangsa yang berada di Malaysia.

Untuk pengetahuan, kod telefon antarabangsa Malaysia bermula dengan +60 dan diikuti dengan nombor telefon. Contohnya +6012xxxxxx . Tetapi SCAMMER dari luar negara ini akan menggunakan kod negara yang berbeza.

Sistem SMS Broadcast ini sebenarnya boleh didapati dengan mudah sebenarnya. Sekiranya anda tahu caranya, mungkin sistem ini boleh didapati secara percuma.

Untuk yang lebih mengetahui tentang aplikasi SMS Broadcast, ia boleh didapati secara percuma. Lakukan sedikit penyelidikan mengenai aplikasi ini nescaya anda dapat menggunakan secara percuma.

Seterusnya, apabila identity pengirim telah dapat digantikan, maka dengan mudah penipuan ini dapat dilakukan. SCAMMER hanya perlu menghantar SMS yang dapat menarik perhatian mangsa.

Contoh SMS yang dihantar adalah banyak. Antara yang paling popular adalah :

"Sekiranya anda ingin memenangi wang tunai sebanyak RM 27,000 sempena Tahun Baru dan ulangtahun Syarikat XXXXXX, Untuk menebus ganjaran anda sila hubungi xxxxxxxx"

"Tahniah, SIM kad anda telah terpilih untuk memenangi hadiah wang tunai RM10,000 dan percutian ke Bali. Sila dapatkan hadiah anda dengan menghantarkan maklumat akaun bank anda ke xxxx"

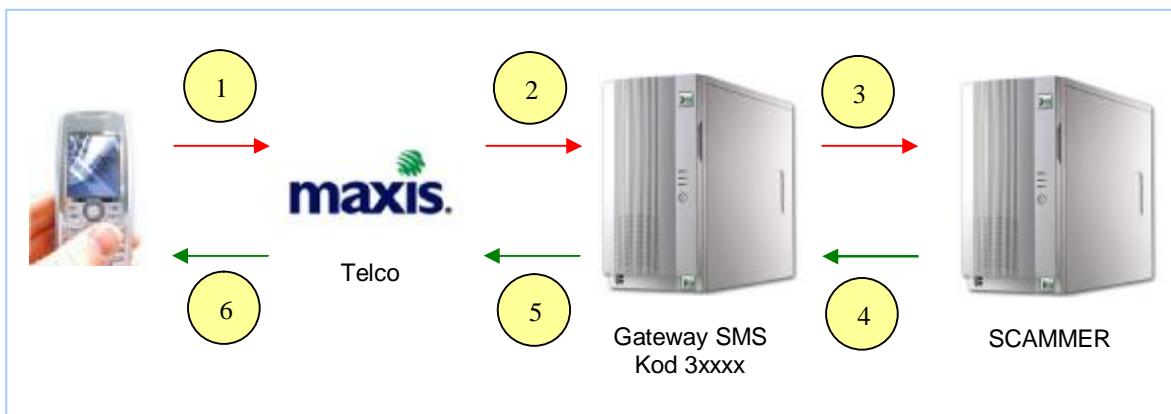
2. Manipulasi SMS Subscribe

Aplikasi kedua yang sering dimanipulasikan oleh SCAMMER adalah dengan menggunakan aplikasi SMS Subscribe.

SMS Subscribe sebenarnya adalah satu aplikasi SMS yang membolehkan pengguna melanggan sesuatu perkhidmatan SMS. SMS Subscribe adalah aplikasi yang popular yang digunakan sekarang dalam perkhidmatan SMS. Ia boleh dikenalpasti apabila format sesuatu SMS itu dimulakan dengan perkataan seperti ON, REG, DAFTAR dan sebagainya. Di kaca televisyen, contohnya adalah seperti ON CINTA, ON KAWAN, REG EPL dan sebagainya.

Kebanyakan perkhidmatan SMS Subscribe yang dijalankan adalah sah mengikut undang-undang tetapi jika disalahgunakan boleh menjadi suatu penipuan.

Mekanisma teknikal SMS Subscribe adalah berbeza berbanding dengan SMS Broadcast. Bagi tujuan pemahaman, sistem SMS Subscribe ini melibatkan beberapa pihak.



Andaikan mangsa pernah melanggan satu perkhidmatan SMS Subscribe. Pelanggan akan menghantar SMS tersebut kepada telco seterus telco akan menghantar nombor pelanggan tadi ke syarikat gateway. Syarikat gateway ini adalah syarikat yang memiliki kod 5 digit seperti 3xxxx.

Seterusnya syarikat gateway akan menghantar nombor telefon tersebut kepada SCAMMER.

Mengapa syarikat gateway bersekongkol dengan SCAMMER ? Sebenarnya syarikat gateway tidak bersekongkol untuk menipu. SCAMMER ini biasanya tidak dikenali oleh syarikat gateway. SCAMMER menghubungi syarikat gateway dan menyewa perkhidmatan SMS Subscribe. Apa yang ingin dilakukan oleh SCAMMER tidak diketahui oleh syarikat gateway.

Penipuan melalui SMS Subscribe boleh berlaku apabila SCAMMER menghantar SMS kepada mangsa tanpa mengikut syarat dan terma penghantaran yang dipersetujui mangsa.

Contohnya apabila pelanggan menerima banyak SMS berulang secara sengaja yang dihantar oleh SCAMMER. Kadang kala SCAMMER menghantar SMS yang lebih dari jumlah yang dipersetujui oleh mangsa.

Setiap kali menerima SMS dari SCAMMER, mangsa akan dicaj. Perkara ini boleh berlaku berulang-ulang, lebih-lebih lagi mangsa tidak tahu untuk keluar dari langganan tadi.

3. Manipulasi SMS IOD

Penggunaan SMS IOD yang sebenarnya adalah untuk membolehkan pelanggan meminta sesuatu maklumat dan pelanggan dikenakan caj terhadap maklumat yang diterima. Contohnya seperti memeriksa saman kereta, mendapatkan waktu solat atau undian rancangan reality tv.

Dengan memanipulasikan SMS IOD, SCAMMER boleh menjerat mangsa dengan memperdaya dengan perkhidmatan selingan didalam SMS yang dihantar.

Contohnya, pelanggan ingin mengundi rancangan TV Akademi Fantasia.

Jadi pelanggan akan menaip, AFUNDI<jarak>Mawi dan dihantarkan ke 32999.

Setiap undian yang berjaya, pelanggan akan menerima SMS balasan dari Akademi Fantasia. Contohnya :

“ Terima kasih diatas undian anda. Undi anda pasti membantu penyanyi kegemaran anda untuk terus kekal di tempat teratas.”

Kalau kita kaitkan dengan penipuan melalui SMS Subscribe yang diceritakan sebelum ini, SMS IOD juga boleh dimanipulasikan dengan menyelit teks yang mendorong pelanggan untuk melanggan dalam perkhidmatan SMS Subscribe. Contohnya, teks SMS Balas itu ditambah seperti berikut :

“ Terima kasih diatas undian anda. Undi anda pasti membantu penyanyi kegemaran anda untuk terus kekal di tempat teratas. Untuk mendapatkan ganjaran bonus RM2,000, taipkan ON XYZ dan hantarkan ke 3xxxx”

Dengan memasukkan teks tambahan seperti “Untuk mendapatkan ganjaran bonus RM2,000, taipkan ON XYZ dan hantarkan ke 3xxxx”, dengan mudah pelanggan terpedaya dan terdorong untuk melanggan perkhidmatan yang lain pula.

4. Menggunakan Sistem SMS Secara Hybrid

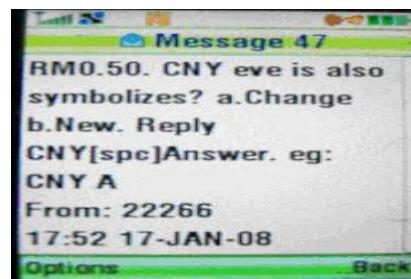
Kaedah yang digunakan adalah lebih licik. Hybrid merujuk kepada campuran pelbagai aplikasi SMS secara serentak untuk penipuan. Ini bermakna SCAMMER menggunakan SMS Broadcast, SMS Subscribe dan SMS IOD secara berselang seli dan bersepada bagi mengaburi mangsa.

Katakanlah, 5 maklumat sehari dan setiap sms dicaj sebanyak RM1.00. Ini bermakna jumlah kutipan dari setiap mangsa adalah sebanyak RM5.00 sehari.

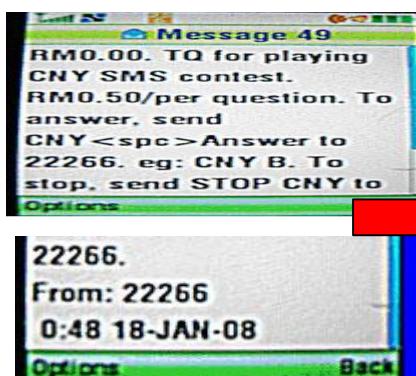
Cuba anda kira sekiranya seramai 10,000 mangsa yang terlibat. Ini bermakna, hasil penipuan mereka dalam masa sehari sahaja adalah sebanyak RM 50,000. Memang licik!



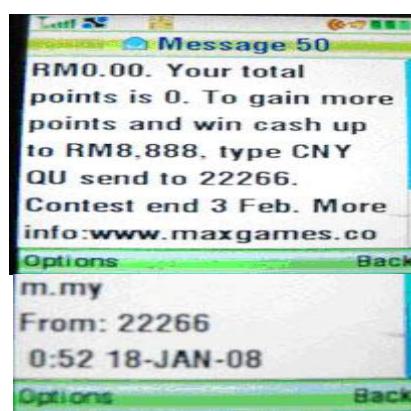
1. SCAMMER menghantar SMS percuma kepada mangsa



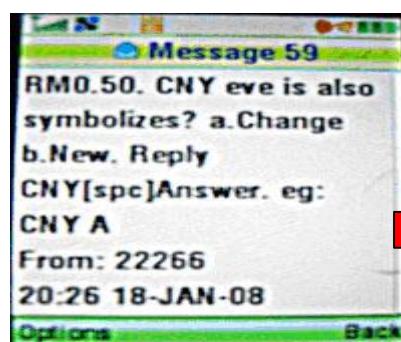
2. Mangsa yang terpedaya akan mendaftar untuk melanggan. Lihat tarikhnya pada 17 Januari 2008



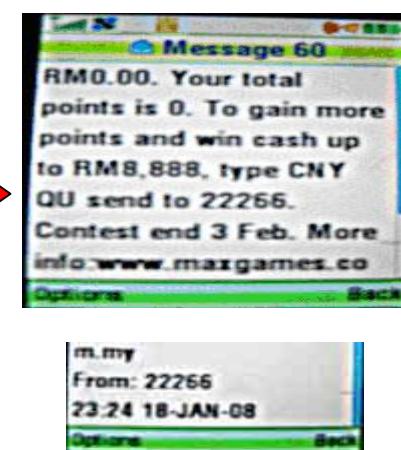
3. SMS Seterusnya Sewaktu Mangsa Tidur Waktu : 00.48 : 12.48 pagi pada 18 Januari.



4. Setiap SMS yang diterima telah dikenakan caj RM0.50



5. Disebabkan mangsa tidak unsubscribe, SMS terus masuk ke telefon & dikenakan caj RM0.50



Adakah Anda Prospek Menjadi Mangsa

1. Sekiranya seseorang sedang menghadapi masalah kewangan yang agak kritikal, mungkin terlihat scam ini satu peluang!
2. Ingin mencuba nasib dan beranggapan bahawa satu anugerah atau "rahmat" telah datang secara tiba-tiba.
3. Andaikan hadiah yang ditawarkan ialah RM 15,000. Mangsa beranggapan bahawa beliau hanya perlu membalias satu sms dengan kos sebanyak RM 0.15 sahaja.
4. Mangsa beranggapan bahawa SCAMMER ikhlas dan jujur kerana meminta maklumat pengesahan terkini sebelum proses pemindahan wang dilaksanakan.

Kaedah Penipuan SMS

Senario #1 : Proses Penipuan :

1. SCAMMER akan menghantar maklumat palsu kepada bakal-bakal mangsa mereka secara rawak samada menggunakan handphone mereka sendiri atau melalui system sms hebahan (broadcast).
2. Kandungan SMS menyatakan bahawa mangsa akan memenangi hadiah, wang tunai atau cabutan bertuah.
3. SCAMMER akan menyakinkan mangsa bahawa tawaran hadiah lumayan tersebut hendaklah diproses secepat yang mungkin. Sekiranya agak lambat, hadiah tersebut dikira lopus dan akan diberikan kepada beribu ribu pelanggan lain yang sedang menunggu.
4. Mangsa akan dikenakan syarat iaitu dikehendaki membayar yuran pemprosesan bagi membolehkan pemindahan wang tunai dilaksanakan.
5. Mangsa dikehendaki membayar yuran pemprosesan tersebut di mesin ATM.

Senario #2 :

Untuk helah kedua, SCAMMER masih menggunakan proses senario pertama tetapi ditukar dari pembayaran melalui mesin ATM kepada pembayaran online banking.

Proses Penipuan :

1. SCAMMER tidak menyatakan apa-apa pembayaran yuran pemprosesan sebaliknya mengarahkan mangsa untuk mendapatkan identiti pengguna dan kata laluan Akaun Internet Banking.
2. SCAMMER berpura-pura menunjukkan keikhlasan membantu mengaktifkan Akaun Internet Banking.

3. SCAMMER hanya meminta 16 digit number yang tertera di Kad ATM mangsa dan No Kad Pengenalan sebagai pengesahan.
4. SCAMMER akan mengarahkan mangsa untuk mengaktifkan ID dan kata laluan di Mesin ATM yang berhampiran.
5. Sewaktu di ATM Mesin, SCAMMER akan memberikan panduan cara-cara mengaktifkan akaun tersebut. Pada masa yang sama, mangsa akan rasa seperti dibantu untuk menguruskan Akaun Internet Banking tanpa meminta apa-apa bayaran.
6. Mangsa akan memasukkan Kad ATM mereka untuk pemprosesan pin number sebanyak dua kali.

Pin pertama adalah pin number yang diperolehi secara sah dari Bank manakala pin number kedua adalah dari mangsa sendiri. Dalam situasi ini, SCAMMER yang akan menyediakan panduan pengaktifan pin number kedua.

7. Pin number kedua tersebut sebenarnya adalah kata laluan untuk Akaun Internet Banking mangsa.
8. Ini bermakna SCAMMER telah mempunyai maklumat lengkap Internet Banking mangsa.
9. Setelah mendapat semua maklumat Internet Banking mangsa, SCAMMER akan memindahkan kesemua wang mangsa ke akaun mereka.

Senario #3

1. SCAMMER akan menghantar maklumat palsu kepada bakal-bakal mangsa bahawa mereka telah memenangi cabutan lottery yang bernilai ribuan atau jutaan ringgit dari luar negara.

2. Pihak SCAMMER memaklumkan bahawa hadiah kemenangan tersebut telah disediakan untuk didepositkan ke akaun anda tetapi terdapat sedikit halangan seperti berikut :

- ü Menurut Akta Bank Negara atau Undang-Undang Bank di Malaysia, syarat untuk mendepositkan wang tersebut hendaklah disertakan dengan pembayaran kadar faedah bank.
 - ü Untuk memudahkan pemahaman mangsa, SCAMMER memberikan contoh proses menunggu pembayaran cheque. Cheque hanya boleh ditunaikan dalam masa 3 hari bekerja.
 - ü Kadar faedah bank yang dikenakan adalah mengikut jangkamasa proses pemindahan keseluruhan dana tersebut ke Malaysia. Ia juga dikenali sebagai "floating rate". Tempoh paling cepat ialah selama satu bulan menunggu.
 - ü Sebagai contoh, untuk proses pemindahan wang dari luar negara sebanyak USD 100,000 (RM320,00) dikira seperti berikut :
 - o Daily Floating Rate = 0.5% sehari = RM1,600
 - o Sebulan - 20 hari bank bekerja
 - o $20 \times 0.5\% = 10\%$
 - o Jumlah keseluruhan untuk sebulan adalah RM 32,000
3. Mangsa yang terpengaruh akan mendepositkan ke akaun SCAMMER kerana dijanjikan bahawa setelah keseluruhan dana sebanyak RM 320,000 dipindahkan, wang pembayaran kadar faedah harian tersebut kekal menjadi milik mereka.
4. Apabila mangsa mendepositkan pembayaran pertama, SCAMMER akan terus menipu dengan menyatakan bahawa mangsa juga telah memenagi cabutan lottery yang kedua.

Berdasarkan tiga scenario SCAMMER di atas, nilai penipuan cabutan lottery adalah nilai yang akan membawa keuntungan yang paling besar kepada SCAMMER.

Kes-kes Yang Melibatkan Penyedia Gateway

1. **Radius Ed Sdn Bhd didapati bersalah** atas aktiviti menghantar sms yang tidak diminta oleh pelanggan dengan niat meraih keuntungan iaitu ‘spamming’. Sebanyak 7 shortcode pihak Radius Ed Sdn Bhd telah digantung perkhidmatan selama 6 bulan bermula dari 21Jun sehingga 6 November 2006. Syarikat Radius Ed juga dikenakan saman.

2 **Unrealmind Interactive Berhad** didapati bersalah kerana tidak menghentikan system sms langganan automatik dan meletakkan harga yang tidak menentu kepada pelanggan. Sebanyak 3 shortcode telah digantung perkhidmatan selama 3 bulan berkuatkusa daripada 21 July sehingga 21 October 2006.

3 Malaysian Allied Mobile Sdn Bhd didapati bersalah atas aktiviti ‘spamming’. Satu short code mereka telah digantung perkhidmatan selama 1 bulan, berkuatkusa daripada 30 Jun sehingga 21 July 2006.

4 MCCM Media Technology Sdn Bhd didapati bersalah kerana tidak menghentikan system sms langganan automatik. Satu short code mereka telah digantung perkhidmatan selama 4 bulan, berkuatkusa daripada 24 July sehingga 16 November 2006.

5 Neurolight Sdn Bhd didapati bersalah kerana tidak menghentikan system sms langganan automatic, masalah keyword, tiada maklumat harga dan cara pengiklanan yang tidak jelas. Satu short code mereka telah digantung perkhidmatan selama 3 bulan, berkuatkusa daripada 13 September sehingga 06 December 2006.

6 Ace Serve Anaconda Sdn Bhd didapati bersalah kerana tidak menghentikan system sms langganan automatik dan satu short code mereka telah digantung perkhidmatan selama 2 minggu berkuatkusa daripada 14 September sehingga 27 September 2006.

7 Parade Nine Techno Sdn Bhd didapati bersalah kerana masalah pengurusan pembaharuan dan 1 short code mereka telah digantung perkhidmatan semenjak 10 January 2007.

8 Rentak Setia Sdn Bhd didapati bersalah atas aktiviti 'spamming'. Satu short code mereka telah digantung perkhidmatan selama 1 bulan, berkuatkuasa daripada 7 March sehingga 6 April 2006.

9 Sealord Technologies Sdn Bhd didapati bersalah atas aktiviti 'spamming'. Satu short code mereka telah digantung perkhidmatan selama 2 minggu berkuatkuasa daripada 3 Mac sehingga 12 Mac 2006.

10 Sybase 365 Asia Sdn Bhd didapati bersalah atas aktiviti 'spamming'. Sebanyak 23 short code mereka telah digantung perkhidmatan selama 3 minggu berkuatkuasa daripada 20 Mac sehingga 17 April 2006.

Ini sebenarnya menunjukkan beberapa usaha telah diambil untuk membentuk salah laku dalam mengendalikan sistem SMS. Dari semasa ke semasa setiap kesalahan akan diambil tindakan yang sewajarnya.

Tidak dinafikan berlaku beberapa kelemahan teknikal terhadap sistem SMS, tetapi perkara ini sentiasa diperkemas oleh pihak syarikat gateway dan telco.

KESALAHAN BERULANG DARI PENYEDIA PERKHIDMATAN

1 T-Force Technology Sdn Bhd

Kesalahan 'Spamming'

Short code 36511 telah digantung perkhidmatan selama 3 bulan berkuatkuasa dari 16 July sehingga 4 Oktober 2006.

Kesalahan Transaksi

Tidak menghentikan system sms langganan automatik dan short code 36511 telah digantung perkhidmatan selama 3 bulan berkuatkuasa dari 12 December 2006 sehingga 12 Mac 2007.

2. Mobile 365 Sdn Bhd

Kesalahan Transaksi

Kesalahan Pertama

Tidak menghentikan system sms langganan automatik dan short code 32120 telah digantung perkhidmatan selama 7 minggu berkuatkuasa dari 3 November sehingga 22 December 2006.

Kesalahan Kedua

Tidak menghentikan system sms langganan automatik dan short code 32130 telah digantung perkhidmatan selama 5 minggu berkuatkuasa dari 16 November sehingga 22 December 2006

3. Macro Kiosk Berhad

Kesalahan Transaksi

Kesalahan Pertama

Tidak menghentikan system sms langganan automatik dan short code 33380 telah digantung perkhidmatan selama 1 bulan berkuatkuasa dari 24 Julai sehingga 25 Ogos 2006.

Kesalahan Kedua

Tidak menghentikan system sms langganan automatik dan short code 36116 dan 36226 telah digantung perkhidmatan selama 2 minggu berkuatkuasa dari 7 Ogos sehingga 22 Ogos 2006

Kesalahan Ketiga

Tidak menghentikan system sms langganan automatik dan short code 32400 telah digantung perkhidmatan semenjak 31 Oktober 2006.

4. Nextnation Network Sdn Bhd

Kesalahan Transaksi

Kesalahan Pertama

Tidak menghentikan system sms langganan automatik dan short code 32099 dan 36226 telah digantung perkhidmatan selama 1 minggu berkuatkuasa dari 20 November sehingga 8 December 2006.

Kesalahan Kedua

Tidak menghentikan system sms langganan automatik melibatkan short code 32099. Ia telah digantung perkhidmatan selama 1 minggu berkuatkuasa dari 21 December sehingga 27 December 2006.

Kesalahan Ketiga

Tidak menghentikan system sms langganan automatik melibatkan short code 32966. Ia telah digantung perkhidmatan semenjak 12 April 2007.

5) Dubaitech Marketing Sdn Bhd

Kesalahan Transaksi

Kesalahan Pertama

Tidak menghentikan system sms langganan automatik dan short code 33566 telah digantung perkhidmatan selama 5 minggu berkuatkuasa dari 24 July sehingga 1 December 2006.

Kesalahan Kedua

Tidak menghentikan system sms langganan automatik dan short code 33522 telah digantung perkhidmatan selama 3 minggu berkuatkuasa dari 27 December sehingga 18 January 2006.

Beberapa Kes Yang Melibatkan Syarikat Ternama

Kes Pertama : Imam Dijerat Skim Hadiah AF 6

Seorang Imam telah terpedaya dengan sindiket penipuan SMS Akademi Fantasia 6 (AF6) yang kononnya dikendalikan oleh Astro dan telah kerugian sebanyak RM 240.00

Imam tersebut menyatakan bahawa sindiket tersebut telah menawarkan hadiah wang tunai sebanyak RM 14,000.00

Beliau telah menyerahkan salah satu maklumat akaun bank kepada sindiket tersebut dan hanya menyedari telah ditipu apabila mendapati baki akaun bank beliau telah berkurangan sebanyak RM 240.00.

Kes Kedua : Amaran Syarikat Shell mengenai Penipuan SMS

Syarikat Shell Malaysia telah memberikan amaran kepada masyarakat umum supaya berwaspada sekiranya menerima maklumat SMS yang menyatakan bahawa mereka telah memenangi suatu pertandingan yang dianjurkan oleh pihak Syarikat Shell.

Pihak Shell menasihatkan masyarakat umum supaya mengabaikan apa jua arahan sindiket penipuan SMS yang meminta mereka melakukan deposit ke akaun bank.

Masalah penipuan ini telah menyebabkan ramai yang menuntut hadiah dari Shell dan Syarikat Petroleum yang lain.

Pihak Shell terus menegaskan bahawa mereka tidak pernah menggunakan SMS untuk berhubung dengan mana-mana pemenang bagi acara pertandingan yang dilaksanakan...

Kes Ketiga : Maxis : Abaikan Penipuan SMS

Menurut Akhbar The Star bertarikh 14 Julai 2007- Sabtu, pihak Maxis menasihatkan masyarakat umum supaya mengabaikan tawaran hadiah kemenangan berbentuk wang tunai ataupun cheque.

Pihak Maxis juga mengingatkan kita supaya mengabaikan mana-mana nombor penghantar SMS yang datangnya dari luar negara atau "short code" yang agak ganjil.

Salah seorang pelanggan menyatakan bahawa :

" Saya telah menerima SMS yang menyatakan telah memenangi cheque tunai sebanyak RM 11,000 daripada Maxis. SMS itu juga mengarahkan supaya saya membuat semakan di laman web sebagai pengesahan memenagi hadiah tersebut"

" Seterusnya, saya telah diberikan satu nombor untuk dihubungi yang terletak di luar negara. Nombor tersebut mengandungi 15 digit. Tanpa rasa curiga, saya telah membuat panggilan ke nombor yang diberikan namun cepat-cepat memutuskan talian tersebut apabila mereka meminta nombor akaun bank saya."

Operator sindiket SMS tersebut juga menyatakan bahawa transaksi pemindahan

Terdapat kes yang sama telah berlaku terhadap Eksekutif bernama Lim tetapi nilai ganjaran yang ditawarkan hanyalah RM 9,000 sahaja.

Encik Lim juga menyatakan bahawa ada menerima promosi SMS yang datangnya dari 5 digit short code dan bukannya dari luar negara.

Beliau juga menyatakan bahawa sekiranya short code tersebut datangnya dari Syarikat Telekomunikasi sekalipun, beliau tetap tidak mempercayainya atas prinsip bahawa bukanlah mudah untuk serta merta menjadi senang atau kaya....

Kes Keempat : Sindiket Penipuan SMS selalunya menggunakan nombor talian luar Negara.



Merujuk kepada terbitan The New Straits Times bertarikh 22 Jun 2008, Encik Ridzuan Zulkifli, Eksekutif Senior Hubungan Media Petronas seperti gambar di atas menyatakan seperti berikut :

" Saya telah menerima panggilan dari seorang wanita Sarawak yang dalam kesedihan kerana telah kehilangan wang simpanannya setelah memberikan maklumat akaun bank melalui talian telefon kepada pihak yang tidak dikenali."

Respon Syarikat Ternama Terhadap Penipuan SMS

Maxis

Pihak Maxis menyatakan bahawa pada bulan lepas, mereka telah menerima sebanyak 100 pertanyaan melalui email : donotdisturb@maxis.com.my mengenai penipuan pertandingan SMS yang menggunakan nama Maxis atau Hotlink sebagai penganjur.

Maxis memandang serius terhadap apa yang telah berlaku dan telah mengambil langkah-langkah yang lebih proaktif dengan menyediakan maklumat-maklumat kesedaran kepada pelanggan mengenai sindiket penipuan SMS ini.

Pada bulan September 2007, Maxis telah memasang peranti anti spam untuk menghalang transaksi sms yang mencurigakan terhadap pelanggan-pelanggan mereka.

Kesan daripada pemasangan peranti tersebut, dianggarkan berjuta transaksi sms yang mencurigakan dapat dihalang dan dikategorikan sebagai spam.

Antara cirri-ciri sindiket penipuan sms ialah segala urusan pertanyaan hendaklah diajukan kepada unit khidmat pelanggan mereka dengan mendail nombor yang telah diberikan. Nombor tersebut bukanlah dari Malaysia sebaliknya terletak di luar negara.

ASTRO

Encik Ahmad Mustaza, Pengarah Unit Khidmat Pelanggan Astro menyatakan bahawa sindiket penipuan sms melakukan penyamaran dengan menggunakan nama syarikat yang mempunyai bilangan pelanggan yang tinggi.

Melalui pengamatan beliau, penipuan sms dirancangkan secara bermusim dan kebiasaanya selaras dengan program-program yang sedang dipromosikan oleh Astro secara meluas seperti program Akademi Fantasia (AF).

Antara penipuan lain yang dikesan adalah sindiket meminta pengguna untuk menyertai pertandingan sim kad Astro.

PETRONAS

Petronas telah menerima panggilan berkenaan pengesahan hadiah kemenangan semenjak tahun 2006.

Menurut Encik Ridzuan Zulkifli, Senior Eksekutif Hubungan Media Petronas, beliau telah mengendalikan sebanyak 1,000 panggilan pelanggan mengenai isu ini dan yang terkini adalah mengenai pertandingan "Petronas Car Craze".

Beliau menyatakan bahawa pemenang-pemenang pertandingan "Petronas Car Craze" akan mendapat maklumat melalui surat rasmi daripada Petronas dan akan dihubungi secara rasmi dari Petronas dan tidak sesekali menghubungi pemenang melalui sms.

Terdapat pengguna yang telah ditipu sebanyak RM 5,000 dan pihak Petronas amat bersimpati terhadap mangsa-mangsa yang telah ditipu.

Pihak Petronas juga telah melaporkan kes-kes penipuan yang telah berlaku kepada pihak polis sebagai langkah pemantauan terhadap sindiket tersebut.

MAYBANK

Pihak Maybank memaklumkan bahawa mereka tidak pernah memohon maklumat peribadi pelanggan melalui sms.

SMS hanya digunakan untuk promosi pemasaran produk dan tidak memerlukan apa-apa maklumat pelanggan.

Bagaimana Menangani SMS Scam

1. Abaikan apa juu tawaran hadiah, wang tunai atau ganjaran yang datang dari SMS.
2. Fahami cara-cara untuk keluar dari sistem SMS Subscribe. Taipkan STOP dan hantarkan ke kod 5 digit.
3. Tapisan maklumat SMS melalui "Anti Spam Toolkit"
4. Baca dan fahami maklumat penting dari Telco anda :
 - a. Maxis :
http://www.maxis.com.my/personal/about_us/announcement/notice.asp
 - b. DiGi
<http://www.digi.com.my/aboutdigi/notices/index.do>
 - c. Celcom
<http://www.celcom.com.my/cep/xresources/CelcomCORP/index.html>
 - i. Sila rujuk ruangan : [About Us > Announcement](#)
5. Membuat aduan kepada pihak berkuasa iaitu :
 - a. Polis
 - b. Suruhanjaya Komunikasi Multimedia Malaysia - Malaysian Communications and Multimedia Commission :
<http://www.skmm.gov.my/>
 - i. Aduan secara e-mail : aduanskmm@cmc.gov.my
 - ii. Telephone : +603-86888000
 - iii. Facsimile : +603-86881880
 - iv. Complaint Hotline : 1-800-888-030

c. [The National Consumer Complaints Centre \(NCCC\)](#)

6. Laporkan kepada Pegawai Syarikat Telekomunikasi yang terdekat.
7. Aduan untuk setiap Telco :
8. Tidak mendedahkan apa-apa jua maklumat Akaun Bank atau Internet Bank anda kepada pihak ketiga walaupun pemanggil atau penghantar sms tersebut menyatakan bahawa beliau adalah wakil dari pihak Bank.
9. Jangan daftarkan TAC (transaction authorisation code) Internet Bank anda dengan menggunakan handphone pihak ketiga. Pastikan daftar dengan handphone anda sendiri.
10. Jangan benarkan mana-mana pihak ketiga menggunakan Kad ATM anda.
11. Berhati-hati bila melaksanakan transaksi online di cyber café kerana terdapat rakaman cctv.

Panduan dan Ingatan Dari Telco

Panduan Dari DiGi

SMS Hoax 1

Public Service Message from DiGi:

We advise our customers to ignore any SMS promising cash rewards and cash prizes from unidentified sources. These SMS are NOT from DiGi. Thank you.

Pesanan Umum daripada DiGi:

Sila abaikan sebarang SMS yang menjanjikan hadiah wang tunai atau sebarang hadiah dari sumber-sumber yang tidak diketahui. SMS ini BUKAN dari DiGi. Terima kasih.

Message 1:

"TAHNIAH!! Sim Card, anda memenangi Peraduan, dari "AKADEMI-FANTASY".
Wang Tunai RM.17,000 Information sila Call; 006285880300678 Terima kasih.
Pengirim; DiGi"

Message 2:

"Congratulations!!! Anda memenangi 1 buah kereta dari DiGi. Info sila hubungi perkhidmatan DiGi 006281399994933. <http://www.digi.com.my>."

Message 3:

"TAHNIAH", SIM CARD ANDA MEMENANGI HADIAH CEK TUNAI RM9000.00 CARI PERADUAN "DIGI" SILA HUBUNGI KHIDMAT PELANGGAN : 006281904077791.
TERIMA KASIH.

Message 4:

"Tahniah Simcard anda memenangi hadiah Cek Tunai dari RM5000 dari AFM Akademi Fantasia Malaysia. Sila hubungi 006281334093111/ 00628133615011 ."

Message 5:

"Tahniah anda memenangi wang tunai RM7000 dari DiGi. Sila hubungi 00628383062988 ."

Message 6:

"congratulations!!! Anda memenangi CEK TUNAI RM11,000.00 dari DiGi. Info sila hubungi perkhidmatan DiGi 006281339662763. <http://www.digi.com.my>"

Message 7:

"You have just won RM9000! You just need to deposit RM1000 cash into this account and the RM9000 will be yours. Bank account xxxxxxxx."

Message 8:

"Tahniah. SIMcard anda telah memenangi hadiah cek tunai RM15,000 plus reload kredit RM250 dari peraduan DiGi. sila hubungi 006281334093111. terima kasih."

Message 9:

"Congratulations! You have won a CASH PRIZE worth RM7,000 from DiGi. Please call DiGi Customer Service at 006281383388204."

Message 10:

"Congratulations! SIM Card Anda Telah Berjaya Memenangi BONUS Cek Bertuah RM15,000 Dari PETRONAS, Sila Call Di Talian 006281319779888 Terima Kasih."

Message 11:

TAHNIAH. Simcard Anda Meme-nangi hadiah cek tunai RM20,000 plus Reload credit 250 dari peraduan DiGi. Sila hubungi Call Centre: 006281241047717 Terima Kasih.

Message 12:

"Congratulation!!! Anda memenangi Cash Cheque RM 20,000.00 from DIGI. Info, sila dail perkhidmatan DIGI; +628 1355 390003, www.digi.com.my"

Message 13:

"Forward from +60160000015 this is DiGi special gift for every DiGi user. Just send this message to another 10 DiGi user and you'll get RM50 free automatic."

Message 14:

"DiGi TELECOMMUNICATIONS SDN BHD, Tahniah!! Simcard Anda dapat bonus RM.17.000, untuk keterangan lanjut sula dil telefon 00006285693774357. Terima kasih." from +6281514324217

Message 15:

"My number Prepaid Anda dapat bonus RM 14.000. >From astro MLYS. Sila dail number office: 0062817705397 Terima kasih."

Message 16:

"My Prepaid Anda berjaya Memenangi Cek, Rm14,000, From astro MALAYSIA. Sila dial number talian 0061817705397. Terimakasih"

Message 17:

"+60162999902 : DiGi is celebrating over 900,000 DiGi holder! Send this message to 9 DiGi holder, you'll receive RM50 free into your cellphone!"

Message 18:

"TAHNIAH.Simcard Anda Meme-nangi hadiah cek tunai RM.20.000 plus Reload credit 250 dari peraduan DIGI.Sila hubungi Call Center : 006281233046639 Terima kasih."

Message 19:

"Congratulatin Anda dapat bonus RM17,000 from "KLCC COMMU" sila dail number office, 006285888288549. T'rimahkasih."

A number: +6281511014036

Perancangan Kerajaan Terhadap SMS Scam

1. Mengkaji dan merangka Akta Spam.
2. Mengkaji cara-cara terkini dan praktikal untuk membentera jenayah sms.
3. Menyediakan system pemantauan terhadap spam.
4. Mendapatkan dan menyediakan tenaga pakar yang mencukupi.
5. Menyediakan policy dan procedure mengenai spam.
6. Menubuhkan unit khas dalam membentera jenayah sms.
7. Melaksanakan siasatan dan tindakan dengan segera.
8. Memberikan panduan dan maklumat kepada pengguna secara berterusan melalui kempen dan media.
9. Menyediakan e-mai aduan sms spam iaitu : spamreview@cmc.gov.my

Rujukan

Maklumat Dari Suruhanjaya Komunikasi & Multimedia Malaysia :

Non Compliance Content Provider, PDF File : [Klik Sini](#)

www.zaharuddin.net

http://www.zaharuddin.net/index.php?option=com_content&task=view&id=715&Itemid=72

The Star 9 Februari 2008

<http://thestar.com.my/news/story.asp?file=/2008/2/9/nation/20283103&sec=nation>

<http://thestar.com.my/news/story.asp?file=/2007/7/14/nation/18303050&sec=nation>

Maxis Anti Spam Toolkit

http://www.maxis.com.my/personal/about_us/announcement/antispam.asp

Jeff Ooi

www.jeffooi.com

Mengenai Penulis



Irwan Dahnil dilahirkan pada 1976 merupakan penulis pertama yang menghasilkan buku panduan perniagaan SMS berbahasa Malaysia. Buku yang bertajuk "Buat Duit Dengan SMS" mula menjadi pembuka mata kepada mereka yang berminat untuk mempelajari perniagaan dan konsep pemasaran SMS.

Irwan Dahnil merupakan founder AkademiSMS.com sebuah laman web yang membantu menyediakan bahan berunsurkan latihan dalam bidang keusahawanan teknologi. Beliau boleh dihubungi di www.irwandalhil.com



Mohd Salleh Esa dilahirkan pada Januari 1975 dan berasal dari Batu Pahat Johor. Setelah melengkapkan pengajian dan bergelar graduan Sarjana Muda Pengurusan Sumber Manusia, beliau telah berkhidmat dalam sektor korporat seperti Petronas, Celcom, Naza dan Road Builder Holding Berhad.

Beliau menegaskan bahawa dalam pengurusan perniagaan dan pemasaran SMS, adalah begitu penting untuk kita menilai kekuuhan kos pemasaran yang berterusan, produktiviti bulanan dan strategi pemasaran yang perlu dilaksanakan.

Untuk apa-apa usahasama perniagaan SMS dengan pihak ketiga, beliau menasihatkan agar jangan mudah terpedaya dengan janji-janji manis dari pelanggan kerana akan menyebabkan anda kerugian yang agak besar.

Mengenai AkademiSMS.com

Menyedari perlunya satu pusat sumber sehenti untuk mendapatkan maklumat mengenai SMS, Akademisms.com diwujudkan. Di dalam laman web ini terkandung maklumat seperti bahan-bahan rujukan untuk memulakan perniagaan SMS, seminar perniagaan SMS dan juga beberapa bahan rujukan lain seperti ebook.

Ebook percuma bertajuk SMS Scam : Penipuan SMS Yang Perlu Anda Tahu adalah salah satu insiatif Akademisms untuk memberi kesedaran kepada masyarakat dalam menangi gejala penyalahgunaan SMS bagi tujuan penipuan.

Dari semasa ke semasa, AkademiSMS. Com akan terus memainkan peranan sebagai agen pemberitahu kepada masyarakat mengenai langkah-langkah yang betul dalam menjalankan perniagaan SMS dengan kos yang paling ekonomi dan risiko yang paling rendah.

Anda boleh melayari www.AkademiSMS.com bagi mendapatkan maklumat lanjut

Satu lagi khidmat masyarakat dibawakan oleh :

