

SCAM: CARA-CARA UNTUK TIDAK TERTIPU (DENGAN PENGETAHUAN UNDANG-UNDANG)

Skim penipuan yang direka untuk menipu seseorang. Biasanya, matlamat utama penipu adalah keuntungan kewangan atau maklumat peribadi. Menurut Gogolook, syarikat teknologi amanah terkemuka, Malaysia kehilangan sejumlah RM 54 bilion (3% daripada KDNK Malaysia) akibat scam dalam setahun. Penyelidikan menunjukkan kira-kira 70% mangsa scam tidak melaporkan kes mereka kepada pihak berkuasa. Berdasarkan artikel daripada Scoop, isu ini telah ditekankan oleh Yang di-Pertuan Agong Sultan Ibrahim Sultan Iskandar di Dewan Rakyat supaya rakyat Malaysia berwaspada dengan jenayah atas talian seperti scam.

EMEL

Anda mungkin menganggap e-mel yang anda terima hanyalah e-mel biasa, tetapi dalam dunia digital hari ini, anda boleh terjebak dengan scam hanya dengan membalas e-mel anda. E-mel scam ini selalunya kelihatan seperti e-mel biasa yang anda terima setiap hari, tetapi sebenarnya maklumat peribadi anda seperti butiran perbankan, kata laluan atau data peribadi yang lain sedang dicuri. Salah satu jenis e-mel scam yang biasa digunakan adalah '*email phishing*'. E-mel jenis ini berpura-pura menjadi organisasi yang sah, menggesa anda untuk bertindak balas dengan cepat.

CONTOH

E-mel Phishing daripada "Bank"–

E-mel yang mendakwa ia daripada bank akan menggesa anda untuk klik pautan bagi melindungi akaun anda atau akaun anda akan disekat.

KWSP atau Penipuan Bayaran Balik Cukai–

E-mel atau panggilan palsu yang menyatakan anda layak untuk pengeluaran KWSP atau bayaran balik cukai LHDN, meminta anda memberikan butiran peribadi.

Scam Cinta–

Scam pada aplikasi temu janji atau media sosial berpura-pura menjalin hubungan sebelum meminta wang kerana "kecemasan keluarga" atau alasan lain.

PANGGILAN TELEFON

Scam melalui panggilan telefon dibuat untuk menipu seseorang untuk mendedahkan maklumat sensitif mereka. Pada masa yang maju ini, setiap rakyat di Malaysia pasti pernah mendapat panggilan scam. Panggilan ini boleh datang melalui telefon peribadi anda ataupun telefon pejabat anda. Scammer biasanya mendapat nombor telefon anda daripada kebocoran data, laman web syarikat anda atau platform media sosial seperti Facebook atau LinkedIn.

CONTOH

Panggilan Telefon daripada "Pegawai Bank"

Pemanggil yang berpura-pura menjadi wakil bank, memberi amaran kepada anda tentang transaksi yang tidak dibenarkan dan meminta butiran perbankan anda untuk "menyelesaikan isu."

Panggilan Polis atau SPRM Palsu

Pemanggil yang berpura-pura menjadi polis, SPRM atau Bank Negara, mendakwa anda terlibat dalam jenayah dan mesti memindahkan wang untuk "tujuan penyiasatan."

Penipuan Amal jariah

Mesej atau panggilan meminta derma untuk badan amal yang menggunakan cerita emosional untuk menekan orang ramai supaya manderma wang.

WHATSAPP

Anda tidak perlu memberikan seseorang nombor telefon anda untuk mereka memilikinya. Hampir semua rakyat Malaysia menggunakan aplikasi WhatsApp untuk berbual tentang hal-hal peribadi, kerja, atau komunikasi bersama universiti kerana ia adalah percuma, cekap dan mudah untuk digunakan. Ini merupakan sebab utama sasaran scammer. Scammer sering mendapat nombor telefon daripada kebocoran data atau platform media sosial.

CONTOH

Scam Penghantaran Bungkus

Mesej atau panggilan yang mendakwa bungkus anda tersekat di kastam atau memerlukan bayaran tambahan sebelum ia boleh dikeluarkan.

Penipuan Tawaran Kerja

Mesej yang menawarkan pekerjaan bergaji tinggi dengan kerja minimum, memerlukan anda membayar "yuran pemprosesan" terlebih dahulu.

WhatsApp di hijack

Seorang penipu yang berpura-pura menjadi rakan atau ahli keluarga, meminta kod pengesahan yang dihantar ke telefon anda untuk mendapatkan akses ke akaun WhatsApp anda.

CARA-CARA MENGESAN SCAM



EMEL



Semak Alamat E-mel (*Spoofing*)

Scammer sering menggunakan alamat e-mel palsu atau mencurigakan yang kelihatan serupa dengan alamat e-mel sebenar. Sentiasa semak e-mel pengirim dengan teliti. Jika ia daripada pihak bank atau syarikat, sahkan e-mel rasmi di laman web mereka. Jika ia daripada seseorang yang anda kenali, hubungi mereka untuk mengesahkan.



Emel sah: moneybank@gmail.com



Emel Scam: m0neybank@gmail.com

Mendesak.

E-mel scam biasanya cuba untuk membuat anda panik. Mereka mungkin mengatakan akaun anda akan dikunci atau anda mesti bertindak segera. Ini adalah helah untuk membuat anda bertindak tanpa berfikir. Pastikan anda bertenang dan sahkan informasi sebelum melakukan apa-apa.

Bahasa dan Tatabahasa yang lemah.

Organisasi yang sah akan menggunakan tatabahasa dan bahasa profesional yang betul dalam e-mel mereka. E-mel scam selalunya mempunyai kesilapan menaip, frasa pelik atau ayat janggal—sesuatu yang orang ramai cenderung untuk terlepas pandang.

Invois Palsu dan Permintaan Pembayaran

Tujuan utama scammer adalah wang. Berhati-hati dengan e-mel yang meminta pembayaran atau invois. Sentiasa semak semula sebelum membuat sebarang pemindahan wang.



PANGGILAN TELEFON



Nombor Tidak Diketahui

Scammer biasanya membuat panggilan daripada nombor yang anda tidak kenali. Mereka melakukan ini untuk mengelakkan pengesanan dan diblok. Berhati-hati jika anda menerima panggilan daripada nombor yang tidak dikenali.

Menyamar sebagai Organisasi Sebenar

Scammer sering berpura-pura menjadi organisasi yang dipercayai seperti LHDN atau bank kerana orang ramai lebih cenderung mempercayainya. Jika anda menerima panggilan yang mendakwa sebagai syarikat atau badan kerajaan, sahkan ia sebelum berkongsi sebarang butiran.

Mewujudkan Rasa Terdesak

Mereka akan cuba membuat anda panik dengan mengatakan terdapat masalah—seperti transaksi yang mencurigakan, bil tidak dibayar atau masalah undang-undang. Matlamat mereka adalah untuk menekan anda supaya bertindak balas dengan cepat tanpa berfikir.

Meminta Maklumat Peribadi

Syarikat yang sah tidak akan meminta butiran perbankan anda, kata laluan atau OTP melalui telefon. Jika pemanggil meminta ini, ia adalah satu penipuan. Letakkan telefon dengan segera.

Gunakan Aplikasi ID Pemanggil

Alat yang berguna untuk membantu mengenal pasti nombor yang tidak dikenali ialah aplikasi Whoscall, yang boleh anda muat turun pada telefon anda. Ia membantu mengesan dan menyekat kemungkinan panggilan scam.

<https://whoscall.com/en>



WHATSAPP



Mesej dari nombor yang tidak diketahui

Scammer akan menghubungi anda daripada nombor yang tidak dikenali. Jika anda menerima mesej daripada nombor yang tidak dikenali, berhati-hati—terutamanya jika mereka meminta butiran peribadi atau wang.

Mewujudkan rasa terdesak.

Scammer akan cuba membuat anda panik dengan mengatakan sesuatu yang mendesak—seperti masalah akaun bank anda, hadiah yang mesti anda tuntutan dengan segera, atau rakan yang menghadapi masalah. Mereka mahu anda bertindak pantas tanpa berfikir.

Menyamar sebagai seseorang yang anda kenali

Helah biasa mereka ialah berpura-pura menjadi rakan atau ahli keluarga yang telah "menukar nombor telefon mereka." Mereka mungkin meminta wang atau maklumat sensitif. Sentiasa sahkan dengan menghubungi rakan tersebut secara langsung sebelum membalas.

Panduan scam WhatsApp

WhatsApp menyediakan sumber rasmi tentang cara mengenali dan mengelakkan scam. Anda boleh mengetahui tentang mesej yang mencurigakan, fail palsu dan cara-cara untuk kekal selamat di sini:

<https://faq.whatsapp.com/2286952358121083>

CARA-CARA ANDA ATAU PEKERJA ANDA DAPAT MENCEGAH SCAM



Latihan Pekerja

Cara terbaik untuk mencegah scam adalah melalui latihan yang betul. Syarikat harus mendidik pekerja tentang mengenali dan bertindak balas terhadap scam.

Mengadakan Bengkel Anti-Scam

Anjurkan bengkel di mana ahli profesional, seperti peguam atau wakil daripada NSRC, boleh mengajar pekerja cara mengenal pasti dan mengendalikan scam. Contoh praktikal dan kes sebenar boleh menjadikan pembelajaran lebih berkesan.

Peringatan

Orang ramai cenderung lupa dari semasa ke semasa. Oleh itu, peringatan harus kerap diberi. Gunakan e-mel atau media sosial syarikat untuk memastikan pekerja mengetahui taktik scam terkini.

Sentiasa berhati-hati

Biasakan pekerja untuk mengesahkan permintaan luar biasa, terutamanya yang melibatkan pembayaran atau maklumat peribadi. Semakan semula dengan jabatan berkaitan boleh mengelakkan kerugian besar.



PERKARA YANG TIDAK PATUT DILAKUKAN



Jangan panik

Perkara paling buruk yang boleh anda lakukan adalah panik. Apabila kita tertekan, kita tidak berfikir dengan jelas, dan itulah yang dimahukan oleh scammer. Tarik nafas dalam-dalam dan balas dengan berhati-hati.

Jangan Terlibat dengan scammer

Sesetengah orang, terutamanya individu yang lebih muda, mungkin menganggap ia menyeronokkan untuk bertindak balas dengan scammer. Tetapi scammer yang mahir pasti akan dapat mengekstrak maklumat tanpa anda sedari—termasuk merekod untuk meniru suara anda. Tindakan paling selamat adalah mengabaikan dan menyekat mereka.

Jangan berdiam diri

Ramai orang berasa malu, takut akan akibatnya, atau menganggap tiada peluang untuk memulihkan kerugian mereka selepas discam. Membuat laporan adalah penting—bukan sahaja untuk potensi pemulihan tetapi juga untuk memberi amaran kepada orang lain dan menghalang scam tersebut daripada berulang.

Dengan mengambil langkah yang betul dan menyebarkan kesedaran, anda boleh membantu melindungi diri anda dan organisasi anda.





UNDANG-UNDANG YANG BOLEH MELINDUNGI ANDA



Akta Komunikasi dan Multimedia 1998 (CMA)

- Seksyen 233: Menangani penggunaan tidak wajar kemudahan atau perkhidmatan rangkaian. Ia menjenayahkan tindakan seperti menggunakan perkhidmatan rangkaian untuk menghantar kandungan palsu, tidak senonoh, lucah atau menyinggung perasaan dengan niat untuk menjengkelkan, menyalahgunakan, mengancam atau mengganggu orang lain.
- Penalti: Pesalah boleh didenda sehingga RM50,000, penjara sehingga setahun, atau kedua-duanya sekali.

Akta Perlindungan Data Peribadi 2010 (PDPA)

- Tujuan: Mengawal pemprosesan data peribadi dalam transaksi komersial, memastikan privasi dan perlindungan data.
- Penalti: Ketidakpatuhan boleh mengakibatkan denda antara RM100,000 hingga RM500,000, penjara satu hingga tiga tahun, atau kedua-duanya sekali.

Akta Jenayah Komputer 1997 (CCA)

- Seksyen 3: Menjenayahkan akses tanpa kebenaran kepada bahan komputer, biasanya dirujuk sebagai "penggodaman."
- Penalti: Individu yang disabitkan kesalahan boleh didenda sehingga RM150,000, penjara sehingga sepuluh tahun, atau kedua-duanya sekali.
- Seksyen 5: Menangani pengubahsuaian tanpa kebenaran kandungan komputer, seperti memperkenalkan '*malware*' atau virus.
- Penalti: Individu yang disabitkan kesalahan boleh didenda sehingga RM100,000, penjara sehingga tujuh tahun, atau kedua-duanya sekali.

Kanun Keseksaan

- Seksyen 416: Meliputi "penipuan dengan penyamaran," yang terpakai pada scam pancingan data yang mana individu menipu dengan berpura-pura menjadi seseorang.
- Penalti: Boleh dihukum penjara sehingga lima tahun, denda, atau kedua-duanya sekali.

Undang-undang ini secara kolektif bertujuan untuk melindungi rakyat Malaysia daripada pelbagai bentuk jenayah siber. Jika anda percaya anda telah disasarkan atau terjejas oleh penipuan siber, adalah penting untuk melaporkan kejadian itu kepada pihak berkuasa yang berkaitan dengan segera.

APAKAH YANG BOLEH DILAKUKAN JIKA EMEL ATAU IDENTITI ORGANISASI ANDA DISALAHGUNAKAN UNTUK SCAM?



Bertenang dan Bertindak Pantas

Menjadi sasaran scammer boleh meresahkan, tetapi panik tidak akan membantu. Perkara penting adalah bertindak balas dengan pantas dan berkesan.

Laporkan Dengan Segera

Jika e-mel atau identiti organisasi anda telah disalahgunakan dalam scam, ambil tindakan segera:

- Hubungi talian hotline bank anda (tersedia 24/7) jika butiran kewangan terlibat.
- Hubungi Pusat Respons Scam Kebangsaan (NSRC) di 997 untuk mendapatkan bimbingan.
- Ikut arahan mereka, yang mungkin termasuk memfailkan laporan polis.

Maklumkan Pekerja dan Klien

Scammer boleh sambung menyasarkan organisasi anda, jadi adalah penting untuk memaklumkan kepada orang lain:

- Beritahu HR untuk mengeluarkan amaran dalaman kepada pekerja.
- Terbitkan notis awam di laman web dan media sosial untuk memberi amaran kepada klien.
- Nasihatkan pekerja supaya lebih berhati-hati dengan e-mel atau panggilan yang mencurigakan.

Dapatkan Nasihat Undang-undang

Jika anda tidak pasti bagaimana untuk mengendalikan keadaan, minta nasihat peguam. Peguam dapat membimbing anda tentang langkah yang perlu dilakukan, seperti mengambil tindakan undang-undang terhadap scammer atau melaksanakan langkah keselamatan siber yang lebih kukuh.



APAKAH YANG BOLEH ANDA LAKUKAN JIKA ANDA DISCAM?

Bertenang dan Proses Situasi Tersebut

- Jangan panik. Scammer bergantung kepada ketakutan dan kekeliruan untuk memanipulasi mangsa. Luangkan masa untuk memproses apa yang telah berlaku.

Laporkan Kejadian dengan Segera

- Jika terdapat penglibatan wang, hubungi talian hotline bank anda dengan segera untuk menyekat transaksi dan melindungi akaun anda.
- Hubungi Pusat Respons Scam Kebangsaan (NSRC) di 997, yang beroperasi setiap hari dari 8 pagi hingga 8 malam, untuk bantuan dalam melaporkan dan mengendalikan kes scam.
- Failkan laporan polis di balai polis terdekat untuk mendokumentasikan scam tersebut dan menyokong sebarang kemungkinan siasatan.

Lindungi Maklumat Peribadi Anda

- Jika anda berkongsi butiran sensitif seperti kata laluan atau maklumat perbankan, tukar kata laluan anda dengan segera dan aktifkan pengesahan dua faktor (2FA) untuk keselamatan tambahan.
- Beritahu majikan anda jika e-mel kerja atau butiran syarikat anda telah terjejas.

Beri Amaran kepada Orang Lain

- Maklumkan kepada rakan sekerja dan klien jika nama, e-mel atau organisasi anda telah disalahgunakan dalam scam untuk mengelakkan mangsa selanjutnya.
- Keluarkan makluman kepada syarikat anda dan notis awam di laman web dan media sosial anda jika perlu.

Dapatkan Nasihat Undang-undang

- Sesetengah scam mungkin melibatkan pencurian identiti, penipuan atau penyalahgunaan maklumat syarikat. Jika anda tidak pasti tentang langkah seterusnya atau memerlukan panduan tentang tindakan undang-undang, nasihat daripada paguam adalah langkah yang paling baik.
- Kami dari Suppiah & Partners bersedia untuk membantu anda. Hubungi kami untuk mendapatkan nasihat undang-undang pakar dan tindakan terbaik untuk melindungi hak anda daripada kejadian tersebut.

Mengambil tindakan segera boleh membuat perubahan dalam mencegah kerugian selanjutnya dan melindungi diri anda atau organisasi anda. Sentiasa berwaspada dan sentiasa sahkan sebelum membalas mesej atau panggilan yang mencurigakan.

RUJUKAN

- **Akta Komunikasi dan Multimedia 1998:** Akta untuk mengadakan peruntukan tentang dan mengawal selia industri komunikasi dan multimedia yang menjurus ke arah percantuman dan perkara-perkara yang bersampingan dengannya.
- **Akta Perlindungan Data Peribadi 2010:** Akta untuk mengawal selia pemprosesan data peribadi dalam transaksi komersial dan untuk mengadakan peruntukan bagi perkara-perkara yang berkaitan dan bersampingan dengannya.
- **Akta Jenayah Komputer 1997:** Akta untuk mengadakan peruntukan bagi kesalahan berhubungan dengan penyalahgunaan komputer.
- **Kanun Keseksaan:** Akta berkenaan dengan kesalahan-kesalahan jenayah.
- **Statistik Scam:** <https://www.malaymail.com/news/malaysia/2024/10/03/scam-epidemic-malaysians-lose-us128b-annually-equivalent-to-3pc-of-gdp-amid-rising-ai-threats/152485>
- **Scoop:** <https://www.scoop.my/news/246047/agong-wants-to-combat-red-tape-culture/>



PEMAKLUMAN PERKHIDMATAN MASYARAKAT INI DIBAWA KEPADA ANDA OLEH:

SUPPIAH & PARTNERS

- 📞 03-4142 3766
- 🌐 <https://suppiahlaw.com/>
- ✉️ thulasy@suppiahlaw.com
general@suppiahlaw.com
- 📍 UG-13, LEXA Galleria,
No. 45, Jln 34/26, Wangsa Maju, 53300 Kuala Lumpur, Malaysia
- 📄 Disediakan Oleh: Adilah Rafi