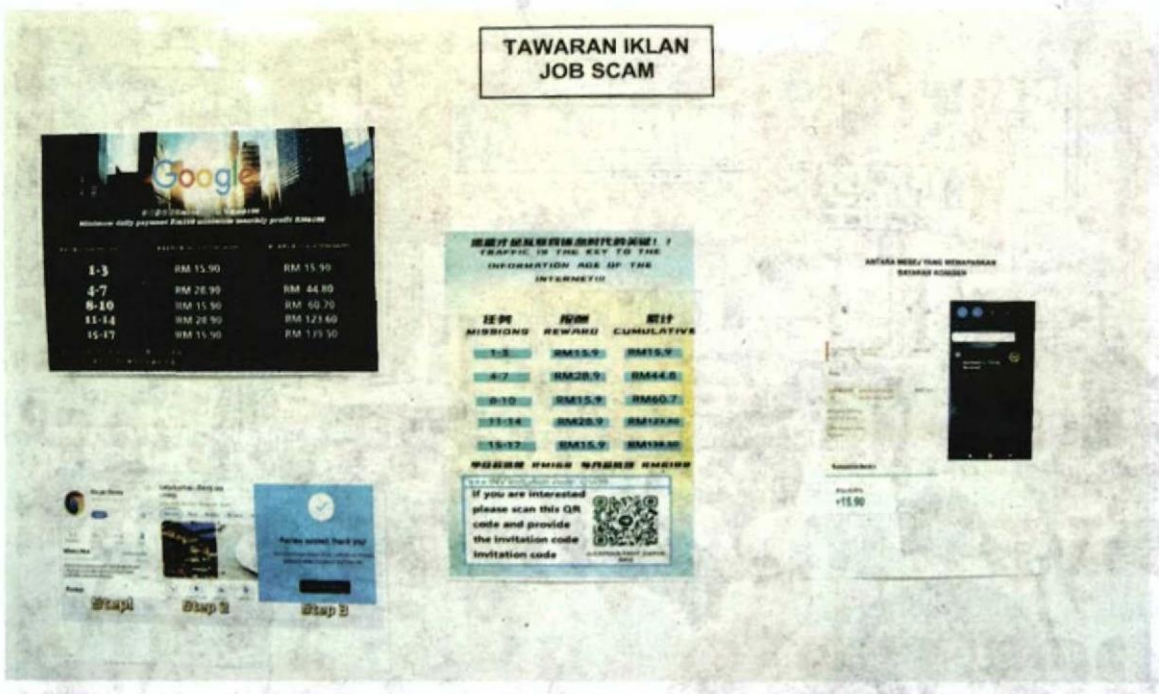
Media Title : Utusan Malaysia
Headline : Penipuan dalam talian berleluasa, semakin canggih dan sukar dikesan
Date : 11 February 2025
Section : General
Page : 16

Penipuan dalam talian berleluasa, semakin canggih dan sukar dikesan

SYAFILA KAMARUDIN



PENTING bagi orang ramai untuk sentiasa berwaspada dan mengambil langkah-langkah pencegahan bagi melindungi diri daripada menjadi mangsa penipuan.

MASALAH penipuan digital di Malaysia semakin membimbangkan apabila ramai rakyat negara ini terus menjadi mangsa pelbagai jenis *scammer*. Sama ada melalui panggilan telefon, mesej teks, atau e-mel, teknik penipuan yang digunakan oleh pihak tidak bertanggungjawab ini semakin canggih dan sukar dikesan. Antara bentuk penipuan yang semakin berleluasa ialah *smishing*, *phishing*, *vishing*, dan juga penipuan melibatkan transaksi dalam talian yang palsu.

Smishing atau penipuan melalui SMS merupakan salah satu bentuk scam yang paling mudah dan berbahaya. Modus operandi penipu adalah dengan menghantar mesej teks yang kelihatan sah, seolah-olah datang daripada bank, agensi kerajaan, atau syarikat telekomunikasi. Mereka akan memanipulasi mangsa untuk memberikan maklumat peribadi atau akaun bank melalui pautan palsu. Akibatnya, mangsa boleh kehilangan wang dan data peribadi mereka dalam sekelip mata.

Phishing adalah salah satu jenis penipuan digital di mana penipu berusaha untuk memperoleh maklumat peribadi atau kewangan mangsa dengan menyamar sebagai pihak yang sah atau dipercayai. Teknik ini biasanya dilakukan melalui e-mel, laman web palsu, atau aplikasi yang kelihatan seperti platform rasmi dari bank, syarikat, atau organisasi yang dikenali.

Penipu yang menjalankan teknik *phishing* biasanya menggunakan pendekatan yang kelihatan sangat meyakinkan. Mereka akan menghantar e-mel atau mesej yang kelihatan datang dari sumber yang dipercayai, seperti bank, perkhidmatan pembayaran dalam talian, atau organisasi kerajaan. Mesej ini sering kali mengandungi pautan yang mengarahkan mangsa ke laman web palsu yang sangat mirip dengan laman web rasmi. Laman web ini direka untuk mengelirukan mangsa agar memasukkan maklumat sensitif seperti nombor akaun bank, kata laluan, nombor kad kredit, dan maklumat peribadi lain seperti nombor kad pengenalan atau tarikh lahir.

Vishing adalah bentuk penipuan yang dilakukan melalui panggilan telefon, di mana penipu menyamar sebagai wakil daripada organisasi atau institusi yang dipercayai untuk memperoleh maklumat peribadi atau kewangan mangsa.

Teknik ini menggunakan taktik psikologi untuk memanipulasi mangsa agar memberikan maklumat sensitif seperti nombor akaun bank, kata laluan, atau butiran kad kredit. Modus operandi *vishing* adalah dengan penipu membuat panggilan telefon yang menyamar sebagai wakil bank, syarikat telekomunikasi, agensi kerajaan, atau institusi lain yang sah.

Penipuan jual beli dalam talian merujuk kepada sebarang tindakan penipuan yang berlaku semasa transaksi jual beli barang atau perkhidmatan di platform e-dagang atau melalui laman web sosial. Dalam jenis penipuan ini, penipu biasanya menawarkan produk atau perkhidmatan yang tidak wujud, menggunakan iklan palsu, atau memberi harga yang terlalu murah untuk menarik mangsa membeli. Apabila mangsa melakukan pembayaran, barangan yang dijanjikan tidak pernah sampai atau kualitinya jauh berbeza dengan yang digambarkan.

Penipuan jual beli dalam talian boleh berlaku dalam pelbagai bentuk, termasuk melalui laman web e-dagang yang sah atau melalui platform media sosial seperti Tiktok, Facebook, Instagram, atau aplikasi mesej.

Adalah penting bagi orang ramai untuk sentiasa berwaspada dan mengambil langkah-langkah pencegahan bagi melindungi diri daripada menjadi mangsa penipuan.

JANGAN TERDESAK

Salah satu teknik utama yang digunakan oleh penipu adalah mencipta rasa kecemasan atau mendesak. Mereka sering menghantar mesej yang memberi amaran palsu seperti mengatakan akaun bank akan dibekukan atau ada aktiviti mencurigakan yang memerlukan perhatian segera. Oleh itu, jangan terdesak untuk bertindak tanpa berfikir panjang. Jika anda menerima mesej atau panggilan yang mendesak, berhenti sejenak untuk menilai situasi tersebut dan pastikan ia sah. Elakkan klik pada pautan atau memuat turun lampiran daripada mesej yang mencurigakan terutama yang mengaku berasal daripada pihak bank atau kerajaan.

PERIKSA NOMBOR PENGIRIM ATAU ALAMAT E-MEL

Sebelum bertindak balas terhadap mesej yang diterima, pastikan anda memeriksa nombor telefon atau alamat e-mel pengirim. Penipu sering menggunakan nombor atau alamat palsu yang kelihatan seperti nombor rasmi bank atau syarikat besar. Anda boleh mencari maklumat tersebut secara manual atau menghubungi pihak yang mengaku menghantar mesej untuk pengesahan. Jika anda tidak pasti, lebih baik untuk tidak membalas mesej tersebut dan mengabaikannya.

GUNAKAN PENGESAHAN DUA FAKTOR (2FA)

Salah satu langkah paling berkesan untuk melindungi akaun dalam talian anda ialah dengan mengaktifkan pengesahan dua faktor (2FA). 2FA menambah lapisan keselamatan tambahan dengan memerlukan pengguna untuk memasukkan dua jenis maklumat yang berbeza semasa log masuk, contohnya kata laluan dan kod yang dihantar ke telefon anda.

Ini akan menyukarkan penyerang untuk mengakses akaun walaupun mereka berjaya memperoleh kata laluan anda. Banyak platform dalam talian penting seperti perbankan dalam talian, e-mel, dan media sosial menawarkan ciri ini untuk meningkatkan keselamatan.

SENTIASA BERHATI-HATI DENGAN TAWARAN YANG TERLALU BAIK

Jika anda menerima tawaran yang kelihatan terlalu baik untuk menjadi kenyataan, itu adalah tanda amaran yang perlu diambil kira.

Penipu sering menggunakan tawaran yang menggoda seperti harga yang sangat murah atau hadiah percuma untuk menarik perhatian mangsa. Sebagai contoh, mereka mungkin menawarkan telefon pintar atau barangan berjenama pada harga yang sangat rendah. Ingat, jika sesuatu tawaran kelihatan terlalu bagus untuk menjadi kenyataan, ia mungkin adalah penipuan. Sentiasa buat kajian lanjut mengenai tawaran tersebut dan pastikan penjual atau laman web yang menawarkan produk itu boleh dipercayai sebelum membuat sebarang pembelian.

Isu penipuan digital termasuk *scammer*, terus menjadi ancaman yang serius kepada masyarakat kita. Dengan taktik yang semakin canggih dan berbahaya, setiap individu perlu lebih peka dan berhati-hati dalam setiap transaksi dalam talian. Adalah amat penting untuk orang ramai mengetahui jenis-jenis penipuan digital ini dan cakna dengan langkah-langkah untuk menghindarinya. Masyarakat harus bekerjasama untuk meningkatkan kesedaran mengenai risiko ini dan perlu mengambil langkah pencegahan yang sewajarnya.

Kita juga perlu sedar walaupun teknologi semakin maju, *scammer* juga semakin kreatif dalam mencari cara untuk menipu orang ramai. Oleh itu, kesedaran dan kewaspadaan setiap individu adalah kunci utama dalam mengelak daripada menjadi mangsa penipuan ini.

Pemeriksaan yang lebih teliti serta tindakan pencegahan yang berkesan dapat membantu mengurangkan risiko kehilangan wang dan data peribadi yang bernilai. Jangan biarkan diri kita terperangkap dalam perangkap *scammer*; sentiasa waspada dan bijak ketika berhadapan dengan dunia digital yang penuh risiko ini.

DR. Syafila Kamarudin ialah Ketua Laboratori Generasi Siber di Institut Pengajian Sains Sosial, Universiti Putra Malaysia.