



Bernama

KAEDAH PENIPUAN MAKIN CANGGIH, TELITI

Kuala Lumpur

Penularan pandemik dan peningkatan penggunaan media sosial memburukkan lagi kegiatan penipuan dalam talian yang hingga kini tidak ada tanda-tanda akan berkurangan, meskipun pelbagai usaha dijalankan oleh pihak berkuasa bagi meningkatkan kesedaran umum tentang jenayah itu.

Berdasarkan statistik Jabatan Siasatan Jenayah Komersial Bukit Aman yang dikongsikan dengan Bernama, jumlah kerugian akibat kegiatan itu yang merangkumi penipuan jualan, pinjaman, pelaburan, telefon serta cinta, meningkat ketara dalam tempoh tiga tahun sejak 2020.

Menurut jabatan itu, pada 2022, rakyat Malaysia kerugian sebanyak RM650,329,897 berbanding RM509,881,921.13 pada tahun sebelumnya dan RM503,883,501.06 pada 2020.

Sementara itu, laporan berita memetik Pengerusi Suruhanjaya Komunikasi dan Multimedia Malaysia Salim Fateh sebagai berkata, jumlah kes kekal tinggi, iaitu kira-kira 12,000 bagi tempoh empat bulan pertama tahun ini.

Kajian yang dijalankan oleh Milieu Insight, firma penyelidikan pasaran dan analisis data Asia Tenggara, membabitkan 2,500 responden di lima buah negara termasuk Malaysia, mendapati hampir separuh rakyat di negara ini pernah disemu daya (tipu daya).

Responden dipilih secara rawak dan mewakili setiap kelompok usia, bangsa dan jantina.

Tinjauan pada 6 Julai itu turut mengenal pasti tipu daya membabitkan penjualan dan pembelian adalah paling lazim, iaitu 39 peratus, penipuan pelaburan (36 peratus) serta jerat pancingan data - mesej melalui e-mel atau platform lain yang disamarkan sebagai sumber benar pada 35 peratus.

Kajian juga mendapati rata-rata mangsa mempunyai tanggapan yang sama tentang jenayah itu.

"Tanggapan 'perkara itu tidak akan berlaku pada aku' adalah antara cabaran paling sukar untuk diatasi... Kita selalu ambil mudah risiko jadi mangsa penipuan," kata Sonia Elicia, Penolong Pengarah Pemasaran Milieu Insight.

Pakar percaya tanggapan bahawa hanya orang yang bodoh, tamak dan naif sahaja akan jadi mangsa penipuan, menyukarkan

Pakar juga pernah jadi mangsa penipuan

orang ramai untuk membentuk serta mengamalkan tabiat dalam talian yang baik dan selamat.

Kaedah penipuan sekarang juga adalah canggih dan teliti, justeru tidak menghairankan jika sesiapa sahaja boleh menjadi mangsa.

Semua pakar yang ditemui oleh Bernama berkata, mereka sendiri pernah menjadi mangsa penipuan dalam pelbagai cara.

Menurut mereka, ada banyak kesilapan biasa yang dilakukan oleh masyarakat semasa di dunia siber yang boleh menyebabkan mereka rentan kepada semu daya.

Kira-kira tiga tahun lalu, ketika pandemik memuncak, Sonia menerima panggilan telefon dan pesanan ringkas, kononnya daripada polis Singapura, menyatakan yang beliau secara teknikalnya telah melakukan jenayah.

Mereka menghantar dokumen berlogo polis Singapura sebagai bukti. Mereka juga mempunyai maklumat peribadinya, membuatkan beliau percaya sedang berinteraksi dengan pegawai penguat kuasa undang-undang.

Mereka meminta beliau membayar SG\$8,000 (RM27,772) bagi menyelesaikan isu terbabit.

"Penipuan berkenaan begitu terperinci membuatkan saya percaya kerana mereka tahu latar belakang saya, siapa keluarga saya, di mana mereka tinggal serta tahu keluarga saya mempunyai anak anjing," katanya kepada Bernama melalui aplikasi Zoom.

Tambah Sonia, penjenayah terbabit mungkin memperoleh maklumat dirinya melalui akaun media sosial beliau.

Pakar bersetuju perkongsian berlebihan mendedahkan orang ramai kepada pelbagai bentuk penipuan seperti Macau Scam dan semu daya cinta.

Faktor yang mempopularkan seseorang di media sosial juga boleh menjadi 'senjata' yang membahayakan orang itu.

"Tidak sukar untuk dapatkan apa sahaja maklumat terperinci daripada media sosial jika seseorang itu terlebih kongsi," kata



JUMLAH kes penipuan kekal tinggi iaitu kira-kira 12,000 bagi tempoh empat bulan pertama tahun ini.

Hazwany Jamaluddin daripada Arus Academy, sebuah organisasi yang mempromosikan pendidikan mampan.

Amnya, orang ramai mempunyai kesedaran untuk tidak mendedahkan maklumat peribadi seperti akaun bank atau alamat rumah, namun, keselamatan dalam talian bukan sekadar melindungi maklumat terbabit, sebaliknya turut merangkumi aspek peribadi lain termasuk perkara yang dianggap tidak penting.

Pakar keselamatan dalam talian menyenaraikan tiga perkara yang begitu mudah dikongsikan oleh orang ramai ketika di alam siber, iaitu foto, lokasi dan keselamatan peribadi.

"Saya paling takut mengenai foto, terutama kanak-kanak. Ramai ibu bapa muda mewujudkan akaun media sosial untuk anak-anak mereka atas alasan mahu dokumentasikan tumbesaran atau perjalanan hidup si anak, sejak bayi.

"Bagi mereka, hal ini bukan satu masalah," kata Kaia Tan daripada Security Matters, sebuah badan bukan kerajaan yang melatih orang ramai tentang kese-

lamatan dalam talian.

Katanya, berkongsi gambar anak kecil dalam talian adalah satu perkara yang tidak selamat kerana berpotensi mengundang perhatian yang tidak diingini.

Hazwany mengesyorkan agar ibu bapa mengaburkan muka si anak jika mereka masih mahu berkongsi foto itu di media sosial, sebaliknya si anak sudah cukup dewasa untuk menguruskan sendiri akaun media sosial mereka.

Jika bukan gambar anak pula, pemilik akaun harus pastikan tidak ada maklumat peribadi atau sulit seperti nombor kad pengenalan atau passport yang boleh membahayakan anda, baik secara fizikal atau kewangan, dalam gambar terbabit.

Satu lagi kesilapan besar yang biasa dilakukan ialah perkongsian lokasi.

Menurut pakar, orang ramai seharusnya berhati-hati apabila tag lokasi mereka di media sosial atau membenarkan perkongsian lokasi apabila membuat hantaran di akaun mereka.

"Jika sekali-sekala anda mahu tag seseorang tempat yang anda rasa cantik, itu tak mengapa, namun bukan (tempat yang merupakan

sebahagian daripada) rutin harian anda," kata Tan.

Pengarah Operasi Security Matters Ivan Lai memberitahu Bernama, ramai pengguna media sosial, khususnya generasi muda, suka berkongsi lokasi apabila melancong atau pertama kali mengunjungi sebuah restoran atau ber-santai.

"Kalau mereka hendak berkongsi lokasi itu, lakukan selepas meninggalkan tempat terbabit (sebagai langkah keselamatan)," katanya.

Berkongsi lokasi, selalunya tempat lepak, adalah sebahagian daripada perkongsian berlebihan yang membuka ruang kepada penipu dan penjenayah lain menggunakan maklumat itu untuk mengambil kesempatan ke atas pengguna terbabit.

Hazwany menggambarkan proses itu sebagai sejenis pemprofilan. Katanya, agak mudah untuk membuat profil seseorang kerana manusia adalah makhluk yang mempunyai tabiat.

"Apabila kita pergi ke tempat-tempat tertentu, hal itu menjadi maklumat untuk pemprofilan. Profil ini mendedahkan maklumat peribadi seperti komuniti, tempat lepak, kereta yang digunakan serta siapa rakan lepak pengguna," katanya, menambah ahli masyarakat seharusnya berha-

ti-hati dalam interaksi dengan orang yang dikenali menerusi media sosial.

Sepatutnya sekarang orang ramai sudah tahu yang mereka tidak boleh mengklik sebarang pautan mencurigakan. Akan tetapi hal itu masih berlaku, demikian menurut tinjauan Milieu Insight.

Sonia berkata, mereka mendapati di Malaysia, kebanyakan semu daya berlaku dengan cara mengumpukan mangsa ke laman sesawang palsu yang kononnya menjual produk tertentu, dan bayaran diambil sedangkan produk tidak wujud.

Mangsa juga dijerat sehingga berkongsi maklumat peribadi yang kemudian digunakan untuk pencurian identiti, atau diperdaya untuk mengklik pautan serta memuat turun perisian hasad.

"Kaedah penipuan yang paling banyak digunakan ialah tinjauan atau pertandingan yang memerlukan maklumat peribadi dan *catfishing*, iaitu penipu menggunakan gambar orang lain dengan identiti palsu dan berkawan dengan mangsa dengan niat mencuri wang, maklumat peribadi serta lain-lain perkara yang berharga," katanya menerusi e-mel.

Tambah beliau, rakyat Malaysia paling banyak ditipu menerusi media sosial seperti Facebook dan TikTok yang lazimnya melibatkan pencurian identiti.

Selain itu, tinjauan juga mendapati seorang daripada empat warga Malaysia, kebanyakannya warga emas, ragu-ragu dalam mengenal pasti nombor atau laman sesawang palsu.

Ada cara untuk melindungi diri serta 'membersihkan' jejak dalam talian pengguna.

Bagi mengenal pasti panggilan penipuan, pakar mengesyorkan penggunaan aplikasi mengenal pasti identiti pemanggil seperti *Whoscall* dan *Truecaller*.

Versi percuma kedua-dua aplikasi ini mengumpul nombor telefon yang telah dikenal pasti sebagai nombor penipuan dan memberi amaran kepada pengguna jika ada yang menggunakan nombor itu.

Pakar juga menekankan kepentingan ciri penyulitan, iaitu proses mengubah data kepada kod serta mengambil tahu platform mana yang menawarkan ciri itu. WhatsApp dan Signal mempunyai ciri penyulitan hujung ke hujung, bermakna tidak ada pihak lain, kecuali si penghantar dan penerima, boleh melihat mesej yang dihantar.

“Tidak sukar dapatkan maklumat daripada media sosial Sonia”