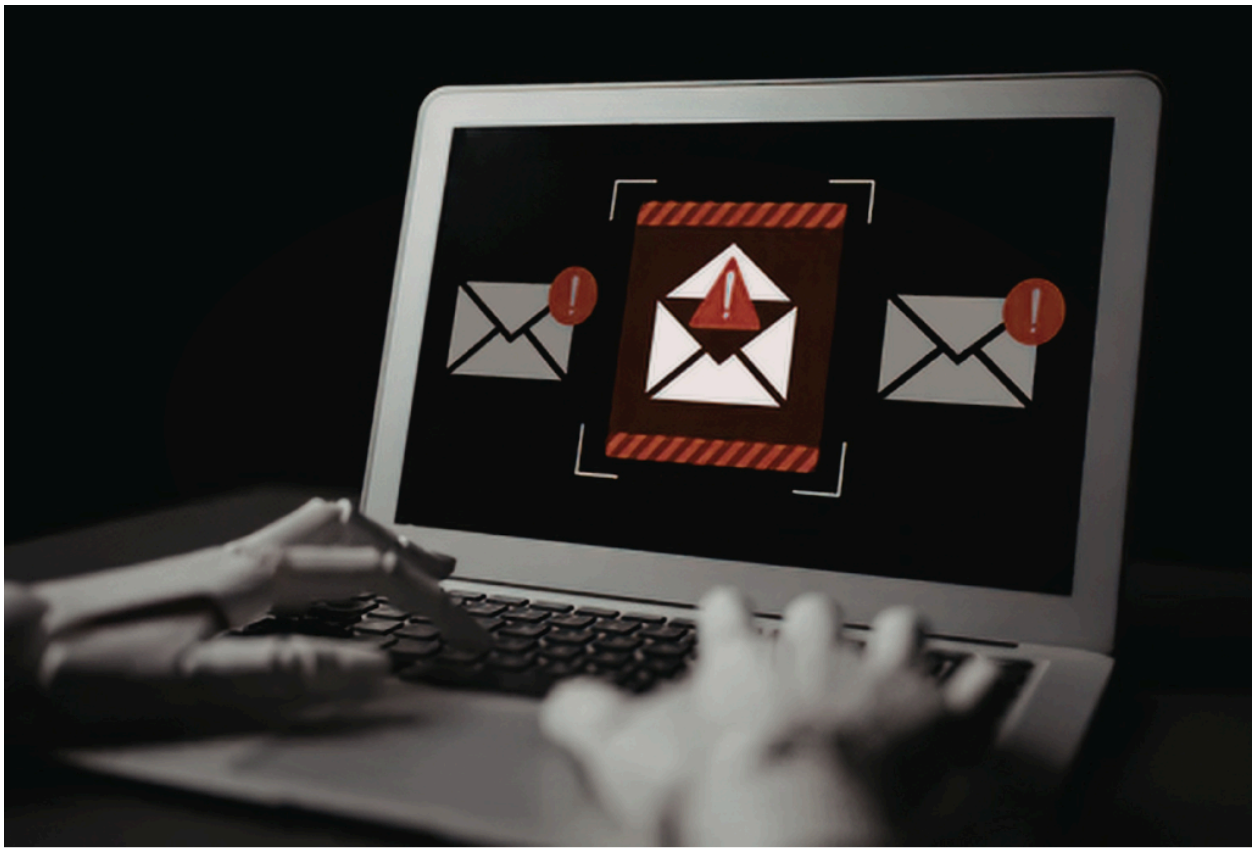
Penipuan Dalam Talian:
Cara-Cara Melindungi Diri Anda Dari Tertipu



Seiring dengan perkembangan teknologi yang semakin pesat, rakyat kini semakin bergantung pada platform digital untuk bekerja, membuat pembayaran dan berhubung setiap hari. Walaupun teknologi dapat memudahkan banyak urusan harian, namun, pada masa yang sama, ia juga menjadikan kita lebih terdedah kepada ancaman dan penipuan dalam talian. Penipuan zaman sekarang bukan lagi sekadar mesej *"Tahniah, anda menang hadiah!"* seperti dahulu. Kini, anda boleh menjadi sasaran hanya kerana anda mempunyai alamat e-mel, akaun bank atau profil media sosial.

Jumlah kes penipuan dalam talian juga tidak menunjukkan tanda-tanda semakin perlahan. Walaupun selalunya warga emas yang dianggap sebagai golongan paling mudah menjadi sasaran, kini kes yang melibatkan golongan anak muda juga semakin meningkat, terutamanya melalui platform yang digunakan setiap hari. Berikut adalah beberapa jenis penipuan dalam talian yang paling sering berlaku, serta langkah-langkah yang anda boleh ambil untuk melindungi diri sebelum terlambat:

1. Penipuan Telekomunikasi: Pemalsuan Tulen (*Deepfake*) & Pemancingan Data Melalui Pemalsuan Suara (*Voice Phishing*)

Penipu kini menggunakan kecerdasan buatan atau *artificial intelligence (AI*) untuk menyamar sebagai orang sebenar seperti pegawai kerajaan, ahli keluarga, dan lain-lain.

Teknologi pemalsuan tulen (*deepfake*) boleh meniru suara dan wajah seseorang dengan cara yang meyakinkan. Anda mungkin akan menerima panggilan daripada orang yang menyamar sebagai salah seorang ahli keluarga untuk meminta bantuan kewangan dengan segera, atau "pegawai kerajaan" yang mendakwa anda terlibat dalam kes undang-undang dan mengarahkan anda memindahkan wang serta-merta untuk menyelesaikan perkara tersebut.

Taktik seperti ini bergantung pada rasa panik dan desakan supaya mangsa tidak sempat berfikir secara rasional.

Cara melindungi diri anda
• **Tunggu sebelum bertindak:** Penipu biasanya menggunakan kata-kata seperti *"segera", "tindakan undang-undang*" atau "*kecemasan*" untuk mencetuskan rasa panik. Jangan lupa, pihak berkuasa yang sebenar tidak akan memaksa anda membuat bayaran serta-merta. • **Pengesahan melalui saluran lain:** Jika terima panggilan daripada "ahli keluarga" yang meminta wang, hubungi nombor sebenar mereka untuk pengesahan. Jika individu tersebut mendakwa dirinya adalah wakil pihak berkuasa atau agensi kerajaan, terus hubungi organisasi berkenaan melalui saluran rasmi seperti e-mel, nombor telefon atau laman web.

2. Tawaran Palsu dan Promosi yang Indah Khabar daripada Rupa

Penipu cukup pantas mengambil kesempatan daripada trend dan isu-isu yang sedang menjadi perhatian ramai. Sama ada tiket konsert, tempahan eksklusif atau promosi terhad, tawaran palsu biasanya direka untuk menimbulkan rasa teruja dan terdesak..

Sebagai contoh, dalam beberapa bulan pertama selepas pembukaan restoran popular Rembayung, ramai telah menjadi sasaran penipuan slot tempahan palsu. Ada yang membuat bayaran kerana menyangka tempahan tersebut adalah yang sah; rupa-rupanya mereka ditipu.

Penipuan seperti ini berkesan kerana ia relevan dan berlaku selari dengan isu semasa. Apabila sesuatu perkara sedang hangat diperkatakan, orang lebih senang percaya.

Cara melindungi diri anda

• **Jangan buat keputusan terburu-buru:** Tawaran "masa terhad" atau notis seperti seperti "slot terakhir" memang wujud untuk membuat anda bertindak pantas. Ambil beberapa minit untuk menyemak kesahihan tawaran sebelum membuat bayaran.
 	
• **Semak jejak digital penjual:** Perhatikan akaun penjual dengan teliti.
  ○ Bila akaun itu dicipta?
  ○ Adakah komen yang diterima daripada akaun-akaun yang betul atau seperti spam?
  ○ Adakah akaun membuat hantaran di akaun secara konsisten?
  ○ Berhati-hati dengan akaun yang baru dicipta atau mencurigakan
 	
• **Cari maklumat sebelum membuat keputusan:** Semak tawaran, penjual atau acara tersebut dengan membuat carian yang dipadankan dengan kata kunci seperti "*scam*", "penipuan" atau "review". Jika orang lain pernah menjadi sasaran, ada kemungkinan besar anda akan jumpa amaran..
 	
• **Gunakan kaedah pembayaran yang selamat:** Elakkan membuat pemindahan secara langsung (*direct transfer*) kepada individu yang tidak dikenali. Jika boleh, gunakan platform yang menawarkan perlindungan kepada pembeli.

3. Penipuan Menggunakan Perisian Perosak (*Malware)* Tersembunyi

Bukan semua penipuan melibatkan pemindahan wang secara langsung. Ada juga yang direka untuk menyusup ke dalam peranti anda secara senyap dan mencuri maklumat tanpa anda sedari.

Ini dikenali sebagai penipuan *malware*, iaitu perisian perosak yang berbahaya yang disembunyikan dalam pautan, lampiran, aplikasi atau fail muat turun. Apabila dipasang (*install)* pada telefon atau komputer, perisian ini boleh menjejaki aktiviti anda, mengakses fail peribadi, merakam kata laluan, malah memantau sesi perbankan dalam talian.

Perisian perosak tersembunyi boleh muncul dalam pelbagai bentuk, termasuk mesej penjejakan penghantaran, amaran perbankan palsu atau pautan untuk memuat turun dokumen.

Cara melindungi diri anda
• **Fikir sebelum tekan:** Jangan buka pautan atau lampiran melainkan anda memang menjangkakannya atau dapat mengesahkan penghantar. • **Periksa mesej yang diterima dengan teliti:** Semak jika ada kesalahan ejaan pada URL atau alamat e-mel, masa penghantaran yang aneh, atau format yang kelihatan janggal. • **Elak membuat muat turun secara tidak rasmi**: Pastikan anda muat turun aplikasi daripada sumber yang dipercayai seperti *App Store* atau *Play Store* yang rasmi. Berhati-hati dengan fail APK atau pautan muat turun daripada pihak ketiga. • **Pastikan peranti ada dikemas kini:** Perisian biasanya dikemas kini dengan tampalan keselamatan (*security patches)* yang melindungi peranti daripada *malware* yang terbaru. • **Bertindak segera jika ada perkara yang mencurigakan:** Jika anda syak bahawa peranti anda terkesan, anda harus tutup sambungan internet, tukar kata laluan yang penting menggunakan peranti yang selamat dan hubungi bank dengan segera jika akaun kewangan anda ada potensi terkesan

4. Amaran Palsu dan Penipuan Data Peribadi

Penipu sentiasa mencari cara helah baru untuk memperdaya mangsa supaya mendedahkan maklumat peribadi dan kewangan, seperti butiran untuk log masuk ke akaun bank, nombor kad kredit atau kad debit anda. Biasanya, helah ini disamarkan dalam bentuk mesej harian yang kelihatan penting atau mendesak.

Contohnya, anda mungkin menerima mesej yang mengatakan mata ganjaran kad kredit anda hampir tamat tempoh, atau kad anda telah digunakan untuk pembelian bernilai besar, seperti “RM3,000 telah dibelanjakan untuk barang kemas”. Mesej itu kemudian akan menggesa anda untuk mengetik pautan atau menghubungi nombor tertentu. Selalunya, maklumat yang diberikan adalah tidak tepat. Contohnya, jumlah mata ganjaran yang salah atau nombor kad yang sebahagiannya ditutup yang bukan milik anda.

Walau bagaimanapun, apabila mesej itu disampaikan dengan nada mendesak, ramai yang terlepas pandang kesalahan-kesalahan tersebut dan terus bertindak. Sebaik sahaja mangsa memberi jawapan, penipu boleh memerangkap mereka untuk

mendedahkan maklumat peribadi dan kewangan. Sebagai panduan umum, bank yang sah di Malaysia tidak akan menghantar pautan yang boleh diklik melalui SMS, jadi berhati-hatilah dengan mesej-mesej sedemikian.

Cara melindungi diri anda
• **Sahkan terus dengan bank anda:** Jangan ketik pautan atau hubungi nombor yang diberikan dalam mesej yang mencurigakan. Sebaliknya, gunakan aplikasi rasmi bank atau cara berhubung yang rasmi untuk menyemak sama ada amaran tersebut benar. • **Semak penyata akaun secara berkala:** Pantau transaksi bank dan kad anda dengan teliti supaya sebarang caj yang tidak sah dapat dikesan dari awal, termasuk langganan atau bayaran iklan yang tidak dikenali. • **Perhatikan butiran yang tidak konsisten:** Beri perhatian kepada butiran kecil seperti nombor kad yang tidak tepat, jumlah bayaran yang pelik atau mesej yang terlalu umum. Ini selalunya petanda penipuan.

Melindungi Ruang Peribadi Anda dalam Dunia Digital

Salah satu aspek pencegahan penipuan yang sering dipandang ringan ialah data peribadi. Semakin banyak maklumat yang dimiliki penipu tentang anda, semakin mudah untuk mereka mencipta taktik penipuan yang kelihatan meyakinkan dan disasarkan khusus kepada anda. Maklumat ringkas seperti nombor telefon, tempat kerja atau rutin harian juga boleh disalahgunakan.

Melindungi ruang peribadi atau privasi bukan sekadar soal keselamatan. Ia juga soal mengurangkan keterdedahan diri kepada penipu. Perkara ini kadangkala diabaikan apabila menggunakan AI untuk kerja atau pembelajaran, seperti berkongsi maklumat sensitif tanpa pertimbangan yang secukupnya. Ketahui cara melindungi diri ketika menggunakan AI melalui panduan kami di sini.

Perlindungan terbaik terhadap penipuan dalam talian adalah lebih daripada sekadar kesedaran, malah sikap sentiasa berwaspada dalam tabiat digital harian juga penting. Jika ada perkara yang rasa “tak kena”, berhenti seketika dan sahkan dahulu. Penipu memang mengharapkan anda mengambil tindakan yang terburu-buru.

Jika anda berdepan situasi mencurigakan atau percaya bahawa anda telah menjadi sasaran, laporkan perkara tersebut kepada pihak berkuasa yang berkaitan. Dengan bersuara, anda bukan sahaja melindungi diri sendiri, tetapi turut membantu orang lain daripada menjadi mangsa.

Ingin mengetahui lebih lanjut tentang jenis penipuan lain? Baca blog kami sebelum ini tentang Penipuan Kerjaya: Kenal Pasti Tanda Amaran dari Awal

Resources

1. https://www.freemalaysiatoday.com/category/leisure/2025/03/26/how-to-protect-yourself-from-online-scams-this-hari-raya
2. https://www.malaymail.com/news/malaysia/2026/04/15/scams-in-the-digital-age-how-hackers-and-ai-are-reshaping-online-fraud-in-malaysia/215123
3. https://dollarsandsense.my/8-common-online-scams-that-malaysians-fall-for/
4. https://www.scoop.my/news/245487/online-scams-in-malaysia-cost-victims-over-rm3-18-billion-in-less-than-three-years/
5. https://www.malaymail.com/news/malaysia/2025/08/04/it-sounded-just-like-my-brother-how-deepfake-voices-are-fuelling-money-scams/183345
6. https://www.bharian.com.my/hiburan/selebriti/2026/03/1520041/daiyan-trisha-dakwa-jadi-mangsa-scam-slot-rembayung