



Elakkan bisnes anda menjadi mangsa scam

Oleh DIANA AZIS

Lindungi perniagaan daripada menjadi sasaran penipuan dalam talian

Jenayah siber termasuk kegiatan penipuan dalam talian di Malaysia ketika ini berada pada tahap membimbangkan sehingga boleh menjadi kritikal sekiranya tidak dibanteras dengan sewajarnya.

Seiring dengan teknologi yang bergerak pantas dan sentiasa berubah, penjenayah alam siber dijangka mampu menyesuaikan diri dengan menggunakan taktik lebih canggih untuk mengeksploitasi kelemahan pengguna serta sistem pertahanan siber pelbagai organisasi di negara ini.

Penipuan dalam talian tidak terhad kepada pengguna komersial malah turut menasaskan perniagaan yang menggunakan platform dalam talian untuk urusan transaksi jualan dan pembelian.

Kebanyakan peniaga yang menjadi sasaran termasuk golongan pengusaha kecil dan sederhana (PKS) yang mungkin baru sahaja menerokai platform dalam talian untuk membangunkan perniagaan mereka.

KENALI TAKTIK LICIK PENJENAYAH SIBER

Para peniaga perlu sentiasa berwaspada dan memainkan peranan mereka dalam melindungi diri dan perniagaan daripada jenayah siber.

Untuk melindungi diri daripada menjadi mangsa penipuan, kenali pelbagai modus operandi yang digunakan oleh penjenayah siber untuk memperdaya mangsa mereka.

Pemalsuan dokumen digital merupakan salah satu modus operandi yang terkenal. Penjenayah siber boleh memalsukan resit atau invoice digital dan mendakwa bahawa mereka telah membeli sesuatu daripada peniaga.

Dengan alasan tidak puas hati, dokumen palsu ini boleh digunakan untuk mempertikaikan sesuatu transaksi dan meminta bayaran balik daripada peniaga, meskipun transaksi tersebut mungkin tidak berlaku.

Baru-baru ini, satu jenis penipuan yang menjadi semakin popular ialah pancingan data. Ia merangkumi teknik seperti penghantaran e-mel palsu, mesej atau mencipta tapak laman sesawang palsu yang kelihatan sah untuk menipu individu supaya memberikan maklumat peribadi atau kewangan mereka. Penjenayah siber boleh memperdaya atau menipu mangsa dengan memperkenalkan diri sebagai pegawai pihak berkuasa, pegawai bank, pegawai mahkamah serta agensi-agensi tertentu dengan tujuan untuk mencuri maklumat peribadi seseorang individu.

Dengan alasan menjual sesuatu produk atau perkhidmatan,

ataupun mendakwa bahawa terdapat bayaran tertunggak, penjenayah menipu mangsa untuk menandatangani wang ke akaun peribadi mereka sendiri.

Penjenayah siber juga akan menyamar sebagai peniaga itu sendiri atau jenama mereka melalui akaun media sosial. Seterusnya, mereka akan menghubungi pelanggan atas alasan menawarkan hadiah percuma dan peluang menyertai peredaran sebagai cara untuk memperolehi data peribadi mereka. Ini merupakan risiko besar kepada reputasi peniaga dan jenama mereka.

Satu lagi taktik pancingan data ialah Kompromi E-mel Perniagaan (BEC), di mana penjenayah menghantar e-mel menyamar sebagai rakan kongsi perniagaan atau pengurus kanan syarikat dan meminta kakitangan syarikat

melakukan pemindahan dana ke akaun bank pihak ketiga yang tidak diketahui.

Selain itu, penjenayah juga menggunakan taktik perisian tebusan atau Ransomware yang merebak melalui e-mel pancingan data yang kelihatan sah, walhal ia mengandungi perisian hasad dalam bentuk lampiran. Perisian hasad merupakan sejenis perisian yang direka untuk mencuri data atau membahayakan sistem komputer.

Jika pengguna memuat turun lampiran berkenaan, penggodam boleh mengakses rangkaian organisasi perniagaan dan data sensitif seperti maklumat pelanggan tanpa had.

Penggodam juga akan menyekat maklumat atau akses tertentu serta menuntut wang tebusan daripada pemilik perniagaan.



BERTINDAK SEGERA SEKIRANYA MENJADI MANGSA JENAYAH SIBER

- Anda perlu segera memaklumkan pihak bank dengan menghubungi talian hotline masing-masing.
- Orang ramai juga boleh menghubungi pusat panggilan setempat 'CCID Scam Response Center' di talian 03-26101559 / 1599. Talian ini beroperasi dari jam 8 pagi sehingga 10 malam setiap hari.
- Anda boleh meminta pihak bank untuk menggantung atau menyahaktifkan akaun anda buat sementara waktu dan pastikan semua dokumen dan butiran berkaitan penipuan yang disyaki disimpan untuk dijadikan sebagai bukti.
- Paling penting, buat laporan polis untuk membantu anda dalam proses penyiasatan!

TIGA LANGKAH TERBAIK UNTUK MELINDUNGI PERNIAGAAN ANDA DARIPADA PENJENAYAH SIBER

Di sini senarai beberapa langkah yang boleh diambil oleh pelanggan untuk melindungi perniagaan mereka daripada dikompromi oleh penjenayah siber.

1. Mempertingkatkan proses pengurusan kewangan perniagaan.

- Wujudkan proses simpan kira yang baik agar dapat meneliti aliran keluar masuk wang setiap bulan dan memastikan tiada kerugian wang yang tidak dijangka.
- Mengesahkan sebarang resit atau invoice yang diterima dengan barangan atau perkhidmatan yang sebenar.
- Berhati-hati semasa memproses dokumen digital mahupun fizikal, pelajari cara-cara mengenal pasti sebarang tanda pemalsuan.
- Gunakan sistem pembayaran digital untuk mengurangkan risiko penipuan.

2. Mewujudkan prosedur dalaman untuk memastikan keselamatan perisian dan rangkaian perniagaan.

- Wujudkan pelayan e-mel peribadi untuk perniagaan anda dan kemaskini perisian untuk semua pekerja.
- Menguatkuasakan perubahan kata laluan yang kerap untuk semua pekerja termasuk akaun media sosial perniagaan.
- Adakan kempen kesedaran untuk mendidik semua pekerja mengenai scam dan taktik pencegahan penipuan.

3. Menjalankan usaha wajar terhadap pihak berkepentingan perniagaan dan pelanggan sebelum berurusan niaga dengan mereka.

- Jangan segera akur dengan sebarang permintaan, terutamanya jika ia melibatkan pemindahan dana ke akaun bank pihak ketiga yang tidak kenali, atau perkongsian butiran peribadi anda.
- Jika anda berasa curiga terhadap permintaan pihak tersebut, minta maklumat yang lebih lanjut berkenaan latar belakang mereka, atau hubungi syarikat yang berkenaan melalui saluran rasmi mereka untuk mengenal pasti kesahihan mereka.
- Bagi pemegang kepentingan perniagaan seperti pelabur, pengesahan boleh dibuat dengan menyemak laman web Suruhanjaya Sekuriti Malaysia.

Artikel ini dibawakan kepada anda oleh CIMB