Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

# Penipuan Ketua Pegawai Eksekutif / Kompromi E-mel Perniagaan

## Apakah Penipuan Ketua Pegawai Eksekutif / Kompromi E-mel Perniagaan?

Penyerang siber terus mengembangkan serangan e-mel yang dipanggil Penipuan Ketua Pegawai Eksekutif (CEO Fraud), atau Kompromi E-mel Perniagaan (BEC). Ini adalah serangan e-mel yang bersasaran dan akan memperdayakan mangsa untuk mengambil tindakan yang tidak sepatutnya. Kebiasaannya penjenayah mahukan wang. Apa yang menjadikan serangan ini sangat merbahaya adalah penyerang siber akan menyelidik mangsa sebelum mereka melancarkan serangan. Ianya juga sangat sukar untuk dihalang oleh teknologi keselamatan kerana tiada lampiran e-mel yang dijangkiti atau pautan hasad untuk dikesan. Begini caranya serangan itu berfungsi.

Penyerang siber menggunakan Internet untuk menyelidik bakal mangsa mereka dan orang-orang yang mereka berinteraksi. Sebagai contoh, jika mereka menyasarkan anda, mereka akan menyelidik siapa bos anda di pejabat atau mungkin juga ejen hartanah yang anda berurusan di rumah. Penyerang siber kemudiannya akan mengarang satu e-mel, menyamar sebagai salah seorang dari individu ini dan menghantar e-mel tersebut. E-mel tersebut sangat mustahak dan memerlukan tindakan secepat mungkin seperti memproses invois, menukar penerima bayaran, atau meyakinkan anda untuk membalas berserta dokumen yang sensitif. E-mel tersebut berfungsi dengan memberikan tekanan kepada mangsa untuk melakukan apa yang mereka mahu. Berikut adalah dua contoh bagaimana serangan tersebut berfungsi.

**Pindahan Wang:** Penjenayah siber mahukan wang, mereka akan menyelidik syarikat anda bekerja seperti mengenal pasti siapa yang bekerja dengan bahagian akaun atau sesiapa yang bertanggungjawab untuk memindahkan wang. Penjenayah kemudiannya akan mengarang dan menghantar e-mel kepada individu-individu ini dengan menyamar sebagai bos atau pegawai atasan. E-mel tersebut akan menceritakan bahawa terdapat kecemasan dan wang perlu dihantar secepat mungkin kepada akaun baru. E-mel tersebut akan memberi tekanan kepada mereka untuk melakukan kesilapan dan realitinya mereka menghantar wang tersebut kepada penjenayah siber.

**Penipuan Cukai:** Penjenayah siber mahukan maklumat peribadi orang ramai untuk melakukan penipuan cukai. Salah satu cara terpantas adalah dengan mencuri maklumat semua pekerja syarikat. Penjenayah akan menyelidik identiti siapa yang bekerja di bahagian Sumber Manusia. Mereka akan menghantar e-mel palsu kepada individu ini dengan menyamar sebagai seorang pegawai atasan atau mungkin juga seseorang daripada bahagian undang-undang. E-mel tersebut dikarang dengan nada mustahak dan maklumat cukai semua pekerja perlu dihantar secepat mungkin. Mereka yang menerima e-mel tersebut menyangkakan mereka menghantar dokumen sensitif kepada pegawai atasan walhal hakikatnya mereka menghantarnya kepada penjenayah siber.

## Melindungi Diri Anda

Jadi apa yang boleh anda lakukan untuk melindungi diri? Pertimbangan akal adalah perlindungan terbaik. Berikut adalah petunjuk lazim untuk dilihat.

**E-mel tersebut selalunya pendek dan mustahak (selalunya hanya beberapa ayat) dan tanda tangan tertulis dihantar dari peranti mudah alih.**

**Mempunyai nada sangat mendesak dan memaksa anda untuk mengabai atau tidak menghiraukan polisi majikan. Sentiasa patuhi polisi dan prosedur berkaitan kerja walaupun e-mel tersebut seperti datangnya dari bos atau pun CEO.**

**E-mel tersebut adalah berkaitan kerja tetapi menggunakan alamat e-mel peribadi, seperti @gmail.com atau @hotmail.com.**

**E-mel tersebut nampak seperti dihantar oleh seorang pegawai kanan, rakan sekerja atau pembekal yang anda tahu sedang bekerja, tetapi nada mesej itu tidak seperti mereka.**

**Arahan pembayaran yang diberikan adalah berbeza dengan apa yang anda terima sebelumnya seperti memohon untuk melakukan pembayaran dengan segera kepada akaun bank yang berbeza.**

Jika anda syak telah menjadi sasaran di tempat kerja, hentikan semua interaksi dengan penyerang dan laporkan kepada penyelia anda. Jika anda menjadi sasaran di rumah atau telah menjadi mangsa dan melakukan pindahan wang, laporkan segera kepada bank, kemudian kepada agensi undang-undang.

## Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

## Editor Jemputan

***Don Cavender*** *adalah bekas ejen khas FBI, dan mempunyai lebih 22 tahun pengalaman dalam forensik digital dan jenayah siber. Baru-baru ini beliau telah menjadi penyelaras untuk menangani organisasi jenayah siber Kompromi E-mel Perniagaan Washington DC. Beliau memberi latihan dan melakukan penyelidikan dalam forensik digital dan penyiasatan siber.* @don_cavender
https://www.linkedin.com/in/donald-cavender

## Sumber

| | |
|---|---|
| Kejuruteraan Sosial: | https://www.sans.org/u/HE3 |
| Hentikan Penipuan Itu: | https://www.sans.org/u/HE8 |
| Hentikan Perisian Hasad Itu: | https://www.sans.org/u/HEd |
| Kunci Log Masuk Anda: | https://www.sans.org/u/HEi |