



Headline: SERANGAN E-MEL PALSU
Publication/Portal: Harian Metro
Date: 14 June 2022

Language: Malay
Section: IT@Metro
Page: 30

SERANGAN E-MEL PALSU

Penyerang siber memerangkap mangsa dengan pembelian atas talian, penstriman hiburan serta sukan kegemaran

FOKUS
Oleh Muhammad Saufi Hassan
saulfia.mediaprima.com.my

Lebih 11 juta e-mel berkaitan pautan meragukan atau 'phishing' disekat membabitkan beberapa negara di rantau Asia Tenggara termasuk

Malaysia. Penjenayah siber pada ketika ini menggunakan kaedah serangan e-mel 'phishing' untuk memerangkap mangsa sama ada organisasi perniagaan atau individu perseorangan.

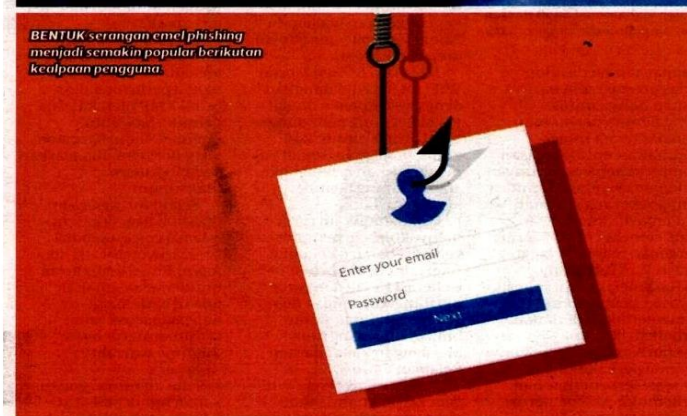
Berdasarkan satu data yang didedahkan oleh Kaspersky menunjukkan bahawa sepanjang tahun lalu sebanyak 11.2 juta e-mel 'phishing' berkenaan berjaya disekat oleh negara Asia Tenggara membabitkan Vietnam, Indonesia dan Malaysia.

Data berkenaan juga menunjukkan bahawa penyerang siber terbabit menggunakan topik popular untuk memerangkap mangsa seperti pembelian atas talian, penstriman hiburan dan sukan kegemaran seperti pautan bola sepak.

Perincian data berkenaan juga memperlihatkan Vietnam menjadi negara paling tinggi yang disasarkan oleh penyerang siber untuk e-mel 'phishing' iaitu 4.01 juta kes diikuti



PENYERANG akan meminta pengguna untuk memasukkan maklumat sensitif kononnya untuk tujuan tertentu sebelum ketirisan maklumat dilakukan pihak tidak bertanggungjawab.



BENTUK serangan emel phishing menjadi semakin popular berikutan kealpaan pengguna.



SERANGAN phishing sering menggunakan pautan topik popular seperti beli belah dalam talian, video penstriman dan hiburan.

oleh Indonesia 2.29 juta, Malaysia (1.79 juta), Filipina (1.33 juta), Thailand (1.28 juta) dan Singapura (0.53 juta).

Pengurus Besar Kaspersky Asia Tenggara, Yeo Siang Tiong berkata, serangan berbentuk e-mel 'phishing' itu semakin popular dalam kalangan penyerang siber.

"Pada masa sama, e-mel ini kekal sebagai medium komunikasi untuk produktiviti dan tugas rutin harian dengan 11 juta cubaan e-mel 'phishing'.

"E-mel juga menjadi platform komunikasi untuk menghantar maklumat kritikal atau berbentuk privasi, sekali gus menjadi sasaran besar untuk penyerang siber memperoleh sasaran dengan mudah.

"Jika kita lihat semula kes e-mel 'phishing' pada 2016, serangan bank di Bangladesh dengan jumlah kerugian RM356 juta dengan sasaran berbentuk e-mel 'phishing,'" katanya kepada #ITMetro.

Siang Tiong berkata, organisasi perniagaan juga perlu memainkan peranan penting dengan mengemas kini setiap tahap keselamatan untuk pelayan utama mereka.

"Secara global, lebih 253.3 juta serangan e-mel 'phishing' direkodkan pada tahun lalu dan sebanyak 8.2 peratus pengguna

menghadapi serangan itu di negara serta rantau berbeza," katanya.

Berdasarkan laporan daripada Verizon, serangan jenis e-mel 'phishing' berkenaan adalah yang kedua paling selalu digunakan oleh penyerang.

Laporan Biro Siasatan Persekutuan (FBI) juga merekodkan serangan terhadap organisasi perniagaan di Amerika Syarikat (AS) bernilai lebih RM8 bilion daripada 2014 hingga 2019.

Kaedah serangan jenis ini memerlukan kepekaan pengguna untuk tidak terperangkap dengan taktik penyerang siber terbabit untuk memperoleh data peribadi mahupun maklumat sensitif.

Kebanyakan pengguna mudah tertipu dengan taktik serangan berkenaan yang banyak mengaitkan dengan topik popular seperti penstriman hiburan atau pautan kononnya daripada data kesihatan.

Serangan menggunakan e-mel 'phishing' berkenaan akan memberikan pautan palsu kepada pengguna sebelum meminta beberapa butiran peribadi pengguna untuk dieksploitasi.

Konsep serangan jenis itu semakin popular pada masa kini kerana ia disifatkan sebagai mudah untuk dilaksanakan berbanding menggodam sesuatu sistem kerangka keselamatan.

Secara global, lebih 253.3 juta serangan e-mel 'phishing' direkodkan pada tahun lalu dan sebanyak 8.2 peratus pengguna menghadapi serangan itu di negara serta rantau berbeza

SIANG TIONG