

Elak Phishing di Internet

Oleh **KHAIRUNNISA SULAIMAN**

“Biasanya laman web palsu yang dibina seakan-akan atau mirip dengan laman bank tempatan bagi memudahkan penipuan.”

SEBELUM bertolak ke kampung di Malaysia Timur, Kamal membuka kotak e-melnya bagi menyemak kiriman terkini yang mungkin memerlukan tindakan pantas.

Jika sudah sampai ke kampung yang tiada kemudahan Internet, memang tidak berpeluanglah dia hendak menyemak dan mengemas kini apa yang patut.

E-mel daripada sebuah bank tempatan yang digunakan majikannya untuk membayar gaji menarik perhatiannya.

Di kotak e-mel tertera Maybank dengan tajuk '1 urgent message'.

Kamal terus klik ke kotak berkenaan, dia bimbang jika akaun banknya digantung sedangkan dia memerlukan wang ketika itu.

Di dalamnya tertulis; Pelanggan yang budiman, anda dikehendaki mengemas kini maklumat akaun bank anda dan TAC diperlukan.

Tanpa rasa curiga dan enggan masalah timbul apabila dia berurusan dengan bank, Kamal terus klik dan mengisi segala maklumat diperlukan serta memberikan nombor TAC seperti diminta.

Dua hari selepas itu semasa dia ke bank untuk mengeluarkan wang, Kamal hampir terduduk apabila mendapati akaunnya hanya berbaki RM3.

Penganalisis MyCert, CyberSecurity Malaysia, Adnan Mohd. Shukor berkata, kisah mengumpun atau phishing bagi mendapatkan maklumat peribadi pemegang akaun bank kini berleluasa bukan saja di negara ini malah di seluruh dunia.

Justeru tegasnya, dua perkara penting yang patut dilindungi oleh pemegang akaun adalah nama pengguna dan kata laluan.

Penjenayah akan sentiasa berusaha mendapatkan nama pengguna serta kata laluan bagi mencerooboh dan mencuri wang pengguna.

Biasanya mereka boleh mendapatkannya dengan meletakkan sesuatu perisian mengintip atau paling biasa menghantar e-mel mengatakan akaun pengguna perlu dikemas kini.

“Jika pengguna tidak peka dan



MyCERT

Malaysia Computer Emergency Response Team



ADNAN MOHD. SHUKOR

membuka pautan berkenaan, mereka akan terperangkap di dalamnya.

“Mereka hanya akan sedar apabila akaun mereka tiba-tiba susut atau tinggal jumlah minimum yang diperlukan bank,” katanya.

Biasanya laman web palsu ini dibina seakan-akan atau mirip dengan laman bank tempatan bagi memudahkan penipuan.

“Jika mangsa tidak peka dengan URL atau alamat bank mereka mungkin akan tertipu dengan mudah,”

katanya. Penipuan menggunakan TAC hanya berlaku jika mangsa dan penjenayah berada di dalam talian pada masa yang sama.

“Penjenayah akan menggunakan nombor TAC yang dimasukkan oleh pengguna di dalam laman web palsu tanpa disedari pengguna,” katanya.

Bagi mengatasi masalah berkenaan, hampir semua bank telah mengambil beberapa langkah keselamatan seperti mengehadkan masa tag digunakan.

Biasanya pihak berkuasa hanya akan bertindak apabila pengguna

melaporkan mengenai laman web bank palsu.

“Perkara ini akan memakan masa yang lama kerana pihak kami perlu menunggu masa untuk menerima laporan,” katanya.

Selepas menerima laporan barulah alamat URL berkenaan disenarai hitam.

Justeru pihak MyCert, CyberSecurity membangunkan perisian plug-in yang dikenali sebagai Don't Phish Me bagi membantu pengguna perbankan dalam talian.

Adnan berkata, perisian yang direka berdasarkan pepadanan laman web perbankan amat mudah digunakan.

“Caranya amat mudah sama seperti memuat turun perisian lain. menggunakan URL bagi Google Chrome:

<https://chrome.google.com/webstore/detail/ekhmajimailpplbglbkopdfjenocpnl> dan Mozilla Firefox: <https://addons.mozilla.org/firefox/addon/dontphishme/>,”

katanya. Adnan berkata, apabila pengguna menerima laman web perbankan yang mencurigakan dan masih belum dilaporkan, perisian Don't Phish Me akan

mengeluarkan amaran di skrin.

Pengguna secara automatik akan diberi amaran manakala pihak Cybersecurity akan menerima laporan secara dalam talian dalam masa yang sama.

Jika pengguna memilih untuk tidak meneruskan pautan berkenaan, satu laman web mengenai Phishing akan terpapar di skrin.

Tetapi jika pengguna masih mahu membuka pautan tadi, amaran akan diberikan bahawa pengguna perlu menanggung risiko sendiri.

Bagaimanapun jika pengguna teruskan hajat tadi, mereka tidak boleh memasukkan nama pengguna kerana laman berkenaan telah disekat.

“Ini memudahkan bukan saja di pihak pengguna tetapi juga CyberSecurity tanpa perlu menunggu laporan pengguna,” katanya.

Bercerita mengenai perisian Don't Phish Me, Adnan berkata, semua bank yang beroperasi di negara ini dilindungi oleh Don't Phish Me.

Senarai bank yang dilindungi oleh Don't Phish Me:

- Maybank2u
- Cimbclicks
- Public Bank
- Bank Rakyat
- Bank Islam
- HSBC
- EON Bank
- UOB
- AMBank
- OCBC
- RHB
- Citibank
- Standard Chartered Bank
- Al Rajhi Bank
- Affin Bank
- Hong Leong Bank
- Alliance Bank

Adnan menambah, pengguna perbankan dalam talian perlu dididik mengenai keselamatan siber supaya mereka berhati-hati apabila berurusan.

“Apa yang paling penting jangan dedahkan nama pengguna dan kata laluan kepada sesiapa saja dan satu lagi jangan buka laman web bank melalui pautan terutama di e-mel,” katanya.

