Siaran Media **16 Jun 2022**

Maybank mengingatkan pelanggan supaya sentiasa berwaspada apabila dalam talian

Bank menyediakan petua keselamatan dalam talian untuk membantu pelanggan melindungi diri mereka

Penipu dalam talian terus mencari cara baharu untuk menipu pengguna yang kurang curiga, terutamanya dengan peningkatan aktiviti e-dagang baru-baru ini yang didorong oleh pandemik COVID-19. Memandangkan lebih ramai pengguna memilih untuk berurus niaga dalam talian pada hari ini, penipu mencari peluang untuk memperdayakan pengguna dengan menggunakan taktik baharu dan canggih.

Selain membangunkan laman web atau aplikasi perbankan palsu untuk memikat atau menarik perhatian pelanggan, penipu kini telah memasukkan komponen 'malware' dalam aplikasi penguatkuasaan undang-undang palsu dan laman web atau aplikasi e-dagang runcit palsu untuk mendapat akses kepada maklumat perbankan dalam talian pelanggan seperti nama pengguna dan kata laluan.

Penipuan biasa yang selalunya menjeratkan mangsa bermula apabila pelanggan menemui tawaran atau iklan murah yang luar biasa di laman web media sosial. Pelanggan kemudiannya menghubungi pembekal/penjual perkhidmatan pihak ketiga (iaitu penipu) untuk mendapatkan maklumat lanjut. Penipu memberikan pautan kepada pelanggan dan memberitahu pelanggan untuk memuat turun aplikasi untuk mengambil bahagian dalam tawaran murah. Apabila memasang aplikasi, pelanggan akan digesa untuk membenarkan aplikasi itu menjadi penyedia perkhidmatan SMS sedia ada. Dengan meluluskan permintaan ini, pelanggan secara berkesan telah memberikan akses TAC perbankan pelanggan kepada penipu untuk kegunaan masa hadapan.

Selepas memasang aplikasi, pelanggan akan diarahkan untuk mendaftar dengan aplikasi yang lazimnya meminta maklumat-maklumat seperti nama, nombor kad pengenalan, alamat e-mel dan nombor telefon, antara lain. Selepas itu, aplikasi akan mengarahkan pelanggan ke gerbang pembayaran palsu (halaman FPX palsu) semasa peringkat pembayaran atau penyempurnaan pembelian. Sebaik sahaja pelanggan memasukkan nama pengguna dan kata laluan dalam halaman ini berdasarkan pemilihan bank pelanggan, halaman tersebut kemudiannya akan menunjukkan mesej ralat bahawa pembayaran tidak berjaya iaitu: ralat yang tidak dijangka berlaku semasa menyambung ke 'server' bank.

Sebenarnya, langkah-langkah ini telah pun menjejaskan butiran akaun perbankan dalam talian pelanggan dengan berkesan kerana penipu kini mempunyai akses kepada nama pengguna dan kata laluan pelanggan, dan juga boleh melihat semua TAC yang diterima oleh peranti pelanggan. Setelah penipu telah mendapat akses kepada butiran ini, penipu akan mula memindahkan dana daripada akaun bank pelanggan dan pelanggan tidak akan sedar kerana mereka telah memberi kebenaran kepada penipu untuk menerima semua mesej SMSnya semasa memasang aplikasi palsu sebelum ini.

Beberapa petua berguna yang boleh diikuti pelanggan untuk melindungi diri mereka apabila menggunakan platform dalam talian termasuk:

- Elakkan memasang/memuat turun fail aplikasi/APK atau klik pada pautan mencurigakan yang dihantar melalui kemudahan chat seperti SMS, WhatsApp, Messenger atau perkhidmatan lain yang serupa.
- Jangan berikan kebenaran untuk mana-mana aplikasi menghantar atau melihat SMS anda.
- Jangan abaikan sebarang amaran daripada peranti anda, terutamanya semasa memuat turun atau memasang fail baharu.
- Jangan masukkan butiran perbankan anda, terutamanya nama pengguna atau kata laluan, dalam mana-mana aplikasi atau laman web yang mencurigakan.
- Sentiasa pastikan perisian antivirus anda dikemas kini untuk perlindungan berterusan.
- Hanya muat turun aplikasi daripada gerbang aplikasi tulen seperti App Store, Play Store atau Huawei AppGallery dan bukan daripada pautan.
- Berwaspada jika anda digesa untuk memuat turun fail yang tidak serasi dengan peranti anda iaitu: Peranti iPhone/iPad diminta menggunakan peranti Android untuk memuat turun fail.
- Sentiasa perhatikan imej dan frasa keselamatan perbankan dalam talian anda (iaitu: imej dan frasa keselamatan Maybank2u), untuk memastikan laman web dan aplikasi adalah sah.
- Jangan ‘root’ atau ‘jailbreak’ peranti anda.
- Kemas kini sistem pengendalian (OS) dan aplikasi peranti mudah alih anda secara kerap.

Jika pelanggan mengesyaki bahawa butiran akaun perbankan dalam taliannya telah terjejas, padam aplikasi dan imbas peranti dengan perisian antivirus. Seterusnya, tukar kata laluan akaun perbankan dalam talian dan hubungi talian hotline penipuan Maybank di +60358914744 untuk bantuan lanjut.

Maybank terus berkongsi kandungan bermaklumat di laman web Maybank2u dan di Facebook dan Instagram, dalam usaha untuk mengingatkan dan mewujudkan kesedaran di kalangan pelanggan tentang bahaya penipuan ‘malware’ ini. Pelanggan harus sentiasa memberi perhatian kepada peringatan ini supaya mereka terus mengetahui tentang kaedah penipuan terkini demi melindungi diri mereka.

Pada masa sama, Bank ingin mengingatkan pelanggan agar terus berwaspada tentang taktik penipuan lain seperti penipuan ‘phishing’ melalui SMS/e-mel, panggilan telefon yang mendakwa pelanggan telah melakukan beberapa jenis kesalahan, pembayaran untuk bungkusan (parcel)

dan sebagainya, yang semuanya bertujuan untuk mendapatkan butiran perbankan pelanggan atau mendorong mereka untuk memindahkan dana mereka kepada penipu.

Bank juga ingin mengesahkan bahawa keselamatan dana pelanggan dan transaksi perbankan dalam talian diutamakan pada setiap masa. Platform dan aplikasi perbankan dalam talian Maybank adalah selamat dan menggunakan kawalan keselamatan yang kukuh untuk memerangi ancaman siber.

Walau bagaimanapun, pelanggan diingatkan untuk memainkan peranan untuk melindungi diri mereka secara berterusan dengan memastikan butiran perbankan dalam talian mereka disimpan selamat dan tidak pernah dikongsi dengan pihak ketiga, sama ada secara sedar atau tidak semasa percubaan ‘phishing’ atau ‘malware’.

Hubungi talian hotline penipuan kami di +60358914744 dengan segera jika anda mengesyaki butiran perbankan anda telah terjejas, kerana ia adalah perkhidmatan talian hotline 24/7 dan Bank boleh membantu anda mencegah kerugian lanjut dengan segera.

****