SECURITY FRAUD ALERT AWARENESS

JANGAN JADI MANGSA PENIPUAN, LINDUNGI AKAUN ANDA!

Kenali jenis penipuan dan bagaimana untuk melindungi diri anda.

PHISING

- Perkataan ‘phishing’ berasal daripada Bahasa Inggeris iaitu password (kata laluan) dan fishing (memancing). Jika digabungkan, perkataan ini membawa maksud memancing kata laluan di mana perkara ini ditujukan ke atas perlakuan meminta, memperoleh atau mencuri kata laluan perbankan internet atau maklumat perbankan anda yang lain tanpa anda sedar.
- Cara-cara melindungi diri anda daripada menjadi mangsa ‘phishing’
- Kebiasaannya mangsa akan ditipu dengan cara mengklik pada pautan palsu yang dihantar oleh penipu melalui e-mel, SMS, WhatsApp, Facebook, Twitter, Instagram dan lain-lain aplikasi. Oleh itu, JANGAN sesekali menekan apa-apa pautan yang diberikan pada anda walaupun maklumat yang dipaparkan menunjukkan penghantar adalah daripada pihak Bank mahupun pihak berkuasa.
- Selain itu, JANGAN memberi maklum balas melalui aplikasi yang dinyatakan di atas terhadap permintaan seperti:
  1) Meminta anda untuk menghantar maklumat peribadi atau perbankan.
  2) Meminta anda untuk mengemaskini ID pengguna, kata laluan, pengesahan imej keselamatan atau soalan keselamatan perbankan anda.
  3) Menyatakan terdapat transaksi yang mencurigakan pada akaun anda atau akaun anda telah disalahgunakan oleh pihak ketiga dan seterusnya meminta maklumat perbankan anda untuk semakan lanjut.

PENIPUAN OTP

- OTP atau one-time password adalah kod 6 digit yang dihantar ke telefon mudah alih anda untuk tujuan pengesahan transaksi yang anda lakukan melalui perbankan internet.
- Penipuan OTP berlaku apabila mangsa menerima OTP untuk transaksi yang tidak dilakukan dan kemudiannya menerima SMS, WhatsApp atau panggilan daripada orang yang tidak dikenali yang menyatakan OTP tersebut adalah untuk mereka yang tersalah hantar ke nombor telefon mudah alih mangsa. Mereka juga kebiasaannya menyatakan bahawa mereka telah tersalah daftar nombor telefon mudah alih mereka dengan nombor telefon mudah alih mangsa. Sekiranya mangsa memberikan OTP kepada mereka, mereka akan berjaya melakukan transaksi pemindahan atau bayaran dengan menggunakan akaun mangsa tanpa disedari.
- Cara-cara melindungi diri anda daripada menjadi mangsa penipuan OTP

- Sekiranya anda menerima SMS, WhatsApp atau panggilan seperti situasi yang dinyatakan di atas, anda dinasihatkan untuk:
  1) JANGAN mudah percaya.
  2) JANGAN dedahkan OTP kepada pihak ketiga atas apa jua alasan atau pujukan.
  3) HUBUNGI pusat khidmat panggilan bank untuk melaporkan kejadian.

PANGGILAN PALSU

- Panggilan palsu berlaku apabila mangsa menerima panggilan daripada orang yang tidak dikenali yang menyamar sebagai pegawai bank, mahkamah, penguatkuasa seperti Polis Diraja Malaysia (PDRM), Suruhanjaya Pencegahan Rasuah Malaysia (SPRM), Lembaga Hasil Dalam Negeri (LHDN) dan lain-lain individu yang berkepentingan. Kebiasaannya, penyamar ini akan menakutkan atau membuat helah kepada mangsa dengan situasi-situasi berikut:
  1) Mangsa mempunyai tunggakan pinjaman atau pembiayaan di bank ataupun tunggakan kad kredit yang tidak pernah dimohon.
  2) Mangsa mempunyai rekod penglibatan dengan urusan jual-beli dadah atau pengubahan wang haram.
  3) Membuat tuntutan insurans/takaful/ubat-ubatan terlarang.
  4) Mangsa mempunyai rekod tunggakan saman atau cukai yang tidak dilunaskan.
  5) Menerima baucar atau hadiah, atau ditawarkan barangan yang murah sehingga tidak masuk akal.
- Mangsa kemudiannya akan merasa takut dan mengikut arahan penyamar tersebut dengan mendedahkan maklumat peribadi, maklumat perbankan mahupun membuat pemindahan ke atas akaun pihak ketiga seperti yang diarahkan. Penyamar akan menakutkan mangsa lagi dengan bertegas akan mengeluarkan waran tangkap ke atas mangsa sekiranya arahan tidak diikut dan meminta keputusan pada waktu kejadian tanpa memberi peluang atau masa untuk mangsa berfikir.
- Cara-cara melindungi diri anda daripada menjadi mangsa panggilan palsu
- Sekiranya anda menerima panggilan seperti situasi yang dinyatakan di atas, anda dinasihatkan untuk:
  1) JANGAN cemas dan mudah percaya.
  2) JANGAN dedahkan sebarang maklumat peribadi dan perbankan anda.
  3) JANGAN mengikut arahan seperti memindahkan wang anda ke akaun pihak ketiga.
  4) JANGAN memuat turun sebarang aplikasi yang diberikan walaupun aplikasi tersebut di atas nama bank atau penguatkuasa seperti Bank Muamalat Malaysia Berhad, Bank Negara Malaysia, Polis Diraja Malaysia dan lain-lain.
  5) HENTIKAN panggilan serta merta sekiranya mencurigakan.
  6) HUBUNGI pusat khidmat panggilan bank untuk melaporkan kejadian.

AKAUN KELDAI/ 'MULE ACCOUNT

Akaun keldai atau nama lainnya akaun tumpang adalah merujuk kepada individu yang membenarkan akaun bank mereka digunakan oleh orang lain untuk transaksi kewangan yang tidak sah atau menyalahi undang-undang.

Selain itu, terdapat juga beberapa situasi lain seperti berikut:

1) Pihak ketiga menghubungi mangsa melalui e-mel, laman sesawang, blog atau media sosial dan menawarkan kerja dalam talian di mana mangsa hanya perlu membuat pindahan wang yang diterima dalam akaun bank mangsa ke akaun bank lain. Mangsa kemudiannya ditawarkan tunai sebagai imbuhan.

2) Pihak ketiga seperti situasi di atas juga boleh menawarkan tunai kepada mangsa sebagai imbuhan untuk membuka akaun bank atas nama mangsa dan menyerahkan akaun bank kepada pihak ketiga tersebut untuk digunakan.

3) Mangsa memohon pinjaman dengan syarikat pinjaman wang berlesen dan telah menyerahkan kad ATM miliknya kepada pihak pinjaman wang berlesen tersebut.

4) Mangsa menyerahkan butiran perbankan dan akaun bank kepada majikan selepas mendapat tawaran pekerjaan.

Untuk makluman, sekiranya anda membenarkan pihak ketiga untuk menggunakan akaun bank anda dan terdapat transaksi-transaksi kewangan yang tidak sah atau menyalahi undang-undang, anda boleh didakwa membantu menyembunyikan harta orang lain walaupun anda tidak sedar akan kesemua transaksi yang dilakukan ke atas akaun anda.

Jangan Kongsi

Elakkan berkongsi maklumat seperti nama pengguna, kata laluan, nombor MyKad anda dan lain-lain melalui e-mel atau ‘pop-up window’ dan panggilan telefon.

Jangan Klik

Sekiranya anda terlihat pautan dalam e-mel, SMS atau ‘pop-up’ sila abaikan dan jangan klik.

Tepat dan Sah

Pastikan laman sesawang yang dilayari adalah sah dan sebaiknya ditaip secara manual bagi mengelakkan anda melayari laman sesawang yang palsu. Pastikan ikon kekunci terdapat di sebelah bar alamat perbankan internet sebelum anda memasukkan nama pengguna dan kata laluan.

Simpan atau Lupus

Pastikan penyata yang dicetak disimpan dengan selamat atau dilupuskan.

Lindung, Sukar dan Tukar

Jangan dedahkan sebarang maklumat perbankan dan kata laluan anda dengan orang lain. Pastikan kata laluan anda unik dan menggunakan gabungan huruf dan nombor, yang menjadikannya sukar untuk diteka. Elakkan menulis kata laluan anda di tempat yang mudah dilihat oleh orang lain atau menggunakan kata laluan yang sama untuk setiap perbankan dan ditukar dengan kerap.

Pantau dan Semak

Sentiasa menyemak dan memantau rekod transaksi anda sekerap yang boleh bagi memastikan tiada sebarang transaksi yang mencurigakan di dalam akaun anda.

Selamat dan Terkawal

Elakkan menggunakan komputer atau rangkaian internet awam yang tidak selamat (public WiFi) apabila melakukan transaksi perbankan dalam talian.

Kemaskini dan Padam

Sentiasa memuat turun versi terkini untuk sebarang aplikasi perbankan internet bagi memastikan anda melayari laman sesawang yang selamat dan sah. Pastikan anda memadam dan mengosongkan ‘cache’ pelayar internet selepas melakukan setiap transaksi perbankan. Fungsi ini berada di bahagian Opsyen / ‘Settings’ pelayar internet anda.

Baca dan Faham

Pastikan anda membaca mesej atau e-mel dengan teliti terlebih dahulu sebelum anda meneruskan transaksi. Sekiranya, terdapat keraguan jangan membalas mesej atau e-mel tersebut.

Sah dan Teruskan

Pastikan log masuk menggunakan imej dan frasa keselamatan milik anda sahaja. Sekiranya anda melihat sebarang imej atau frasa yang bukan milik anda atau imej yang belum tersedia jangan terus memasukkan kata laluan anda.

Berhati-hatilah dengan penipuan kewangan yang menjanjikan pulangan tinggi yang tidak realistik. Sekiranya ia menimbulkan keraguan, sila hubungi:

BNMTELELINK di talian 1-300-88-5465.

CBP Hotline:+ 1-300-88-7650

National Scam Response Centre (NSRC) – 997

Emai : info@cbp.com.my