Siri Artikel: Jadilah Pengguna Kewangan Dalam Talian Yang Bertanggungjawab
Bahagian 1

Selaras dengan perkembangan teknologi dalam perkhidmatan kewangan, risikonya juga turut berkembang. Baru-baru ini, terdapat peningkatan dalam penipuan *malware* melalui telefon pintar, mesej pancingan data (*phishing*), dan penipuan pembayaran dalam talian di rantau ini dan di Negara Brunei Darussalam. Untuk mengatasi ancaman siber ini dan melindungi pengguna-pengguna kewangan, institusi-institusi kewangan secara berterusan mengambil langkah-langkah untuk memperkukuhkan sistem perbankan masing-masing untuk mengelakkan pencerobohan data.

Pada masa yang sama, pengguna kewangan seperti awda juga memainkan peranan yang besar dalam menjaga keselamatan data peribadi serta memperkukuhkan peranti masing-masing. Dengan kerjasama institusi kewangan dan pengguna kewangan, kita boleh membina pertahanan yang kuat dan kukuh untuk menentang risiko kecurian maklumat dan kerugian kewangan, serta memastikan kita sentiasa selamat dalam talian.

Dalam siri artikel empat bahagian ini, kami akan mengongsikan beberapa tip dan nasihat untuk meningkatkan perlindungan daripada penipuan digital dengan menjadi pengguna kewangan di dalam talian yang bertanggungjawab. Pada minggu ini, kita akan membincangkan dengan lebih lanjut mengenai cara-cara untuk melindungi data peribadi awda.

1. Lindungi data peribadi awda

Data peribadi merupakan maklumat atau butiran yang boleh digunakan untuk tujuan pengenalpastian dan pengesahan. Ini termasuk nama penuh, tarikh lahir, nombor kad pengenalan, nombor telefon, alamat perumahan, dan alamat e-mel.

Perkara yang patut dilakukan

- Sentiasa buat pengesahan dengan bank awda melalui saluran perhubungan rasmi mereka untuk mengesahkan samaada panggilan yang diterima adalah sahih daripada mereka.

Perkara yang perlu dielakkan

- Jangan sesekali mendedahkan maklumat atau data peribadi awda melalui telefon atau media sosial. Maklumat tersebut boleh disalahgunakan oleh pencuri identiti.
- Elakkan daripada mengongsikan maklumat dan imej-imej peribadi melalui media sosial yang boleh digunakan oleh penipu atau penjenayah untuk mendapatkan maklumat peribadi awda tanpa kebenaran awda.

Maklumat atau butiran lain yang awda perlu lindungi untuk mengelakkan akses atau penyalahgunaan data oleh individu lain termasuk:

- Nombor akaun bank;
- Butiran kad kredit atau debit, termasuk tarikh mansuh dan kod CVV;
- Butiran perbankan dalam talian atau aplikasi mudah alih, seperti nama pengguna dan kata laluan;
- Mana-mana akaun dalam talian yang digunakan untuk pembelian atau sebagai dompet elektronik;
- Jadual perjalanan dan pas masuk (kod bar boleh mendedahkan maklumat peribadi);
- Resit atau invois terutamanya yang mempunyai kod QR;
- Maklumat dalam label penghantaran atau kiriman untuk sebarang pembelian dalam talian; dan

- Nama-nama keluarga terdekat awda.

Tahukah awda?

Jika awda memberikan atau mengongsikan akses kepada nombor telefon, akaun bank, atau kad debit awda kepada orang lain, awda berisiko terlibat dalam aktiviti yang melanggar undang-undang dan boleh diambil tindakan atas membantu pembersihan wang haram yang merupakan satu kesalahan di bawah Seksyen 3, Perintah Mendapatkan Kembali Aset Jenayah (CARO), 2012. Jika didapati bersalah, awda boleh dikenakan denda tidak melebihi B$500,000 atau penjara selama tempoh tidak melebihi 10 tahun.

Oleh itu, sentiasa berwaspada dan jangan beri maklumat peribadi awda kepada sesiapa yang awda tidak kenali atau percayai.

2. Lindungi barangan fizikal yang mengandungi maklumat sensitif

Memastikan keselamatan barangan fizikal yang mengandungi maklumat sensitif adalah sangat penting kerana aset fizikal dan digital keduanya sering menjadi sasaran oleh penipu dan penjenayah. Barang fizikal ini antaralainnya adalah:

- Buku atau pas akaun bank;
- Kad kredit dan debit;
- Alat-alat peranti termasuk telefon pintar, tablet, komputer riba, atau peralatan elektronik yang digunakan untuk membuat transaksi kewangan; dan
- Token atau alat peranti yang disediakan oleh pihak bank untuk pengesahan identiti.

Perkara yang patut dilakukan

- Pastikan dokumen yang mengandungi maklumat sensitif seperti penyata bank, resit, kad kredit dan debit yang sudah mansuh, dan label penghantaran dibuang dan dimusnahkan dengan sepenuhnya.

Perkara yang perlu dielakkan

- Jangan biarkan barangan fizikal yang mengandungi maklumat sensitif tanpa pengawasan, walaupun untuk tempoh yang singkat. Sentiasa simpan barangan tersebut bersama awda atau di tempat yang selamat.

Amalan-amalan mudah ini boleh membantu untuk memastikan maklumat dan transaksi kewangan awda selamat.

Nantikan artikel seterusnya untuk mendapatkan tip dan nasihat lanjut bagi melindungi diri awda dalam talian pada minggu depan!

Siri ini merupakan inisiatif bersama oleh:
Brunei Darussalam Central Bank (BDCB) (Instagram: @centralbank.brunei),
Pihak Berkuasa Industri Teknologi Info-komunikasi Negara Brunei Darussalam (AITI) (Instagram: @aiti.brunei),
Cyber Security Brunei (CSB) (Instagram: @csb.gov.bn), and
Brunei Association of Banks (BAB) (Laman web: www.bab.org.bn)