

Siri Artikel: Jadilah Pengguna Kewangan Dalam Talian Yang Bertanggungjawab

Bahagian 3

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. Beberapa tip juga akan dikongsikan untuk membina kata laluan yang kukuh.

1. Pantau akaun-akaun awda

Perhatikan akaun-akaun kewangan awda serta akaun-akaun dalam talian yang berkaitan untuk memastikan semua aktiviti dan transaksi adalah betul.

Perkara yang patut dilakukan

- Baca sebarang makluman mengenai akaun bank dan kad awda dengan serta merta.
- Semak penyata bank, penyata kad, dan rekod transaksi secara kerap.
- Hidupkan pemberitahuan untuk memberi amaran bagi sebarang pembelian besar atau transaksi antarabangsa.
- Pastikan awda mengakses laman web yang rasmi atau aplikasi mudah alih yang sah sebelum log masuk dan membuat sebarang transaksi.
- Telefon bank atau pengeluar kad awda dengan menggunakan nombor telefon yang tertera di kad jika awda mengesyaki sebarang aktiviti yang mencurigakan.

Perkara yang perlu dielakkan

- Elakkan daripada menyimpan butiran kad kredit atau debit di dalam laman web atau aplikasi mudah alih.

2. Pastikan kata laluan awda selamat dan kukuh

Kata laluan yang kukuh adalah penting untuk menjaga keselamatan awda dalam talian. Kata laluan yang lemah boleh menyebabkan data awda berisiko mengalami masalah seperti pencurian identiti, kerugian kewangan, dan menjejaskan reputasi. Kata laluan yang kukuh dapat membantu memastikan akaun dalam talian awda sentiasa selamat.

Perkara yang patut dilakukan

- Gunakan frasa laluan yang mengandungi gabungan huruf besar dan kecil, nombor, dan huruf istimewa untuk membuat kata laluan yang unik yang sukar diteka.
- Tukar kata laluan dengan kerap bagi mengelakkan kata laluan dipecahkan melalui tekaan atau pendedahan.
- Aktifkan pengesahan pelbagai faktor atau *multi-factor authentication* untuk semua akaun dalam talian awda.

Perkara yang perlu dielakkan

- Jangan sekali-kali mengongsikan kata laluan awda dengan sesiapa pun!
- Jangan gunakan kata laluan yang sama bagi akaun kewangan awda dan akaun media sosial awda.
- Elakkan daripada menggunakan maklumat peribadi seperti nama, tarikh lahir atau nombor telefon sebagai kata laluan atau PIN.
- Elakkan menggunakan pilihan “simpan kata laluan” dalam aplikasi mudah alih kerana sesiapa yang mempunyai akses kepada peranti awda akan mempunyai akses kepada aplikasi mudah alih itu.

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)