PEMBERITAHUAN

AKTIFKAN PENYAHIHAN DUA-FAKTOR BAGI MENINGKATKAN TAHAP KESELAMATAN AKAUN MEDIA SOSIAL DAN APLIKASI PEMESEJAN ANDA

CYBERJAYA, 10 Februari 2022 --- Suruhanjaya Komunikasi dan Multimedia Malaysia (MCMC) ingin menasihatkan orang ramai supaya mengaktifkan penyahihan dua-faktor *('two-factor authentication'-2FA)* sebagai ciri keselamatan yang membantu melindungi akaun media sosial dan platform pemesejan segera anda selain daripada kata laluan anda.

Statistik trend aduan awam yang diterima oleh MCMC menunjukkan, jumlah aduan berkaitan penggodaman dan kehilangan akses telah meningkat sebanyak 55 peratus, iaitu 1,599 aduan pada tahun 2020 dan 2,483 aduan pada tahun 2021. Rata-rata pengadu memohon bantuan dan nasihat bagi mendapatkan kembali akses kepada akaun dan halaman milik atau kendalian mereka.

Risiko keselamatan sebegini menjadikan penggunaan 2FA lebih mendesak, kerana risiko penggodaman atau pengambilalihan akaun bukan sahaja boleh mengakibatkan kecurian identiti malah boleh membawa kepada penipuan melibatkan kerugian ribuan ringgit.

Lapisan keselamatan pertama secara umumnya adalah gabungan bersama nama pengguna *('username')* dan kata laluan *('password'),* yang telah digunakan sejak awal lagi. Namun, penggunaan kata laluan sebagai satu-satunya langkah keselamatan di alam maya adalah lemah dan terdedah kepada risiko penggodaman atau pengambilalihan akses.

Melalui 2FA, anda akan diminta untuk memasukkan kod log masuk atau kunci keselamatan khas bagi mengakses akaun. Anda juga boleh mendapatkan amaran *('alert')* apabila terdapat percubaan log masuk daripada pelayar atau peranti mudah alih yang tidak dikenali dan diminta mengesahkan percubaan log masuk anda setiap kali terdapat cubaan dibuat.

Sehubungan itu, aktifkan penyahihan dua-faktor bagi akaun anda sekarang. Maklumat lanjut berhubung pengaktifan penyahihan dua-faktor adalah seperti berikut:

1. **Facebook - Login alert and two-factor authentication:**
   www.facebook.com/help/148233965247823/

2. **Twitter – How to use two-factor authentication:**
   https://help.twitter.com/en/managing-your-account/two-factor-authentication

3. **Google 2-step verification:**
   https://www.google.com/landing/2step/

4. **Instagram two-factor authentication:**
   https://help.instagram.com/566810106808145

5. **TikTok – Keep your account secure:**
   https://www.tiktok.com/safety/youth-portal/keep-your-account-secure

6. **Whatsapp two-step verification:**
   https://faq.whatsapp.com/general/verification/how-to-manage-two-step-verification-settings

7. **Telegram – Active Sessions and Two-step verification:**
   https://telegram.org/blog/sessions-and-2-step-verification

8. **Signal PIN:**
   https://support.signal.org/hc/en-us/articles/360007059792-Signal-PIN

Orang ramai juga diminta untuk tidak klik kepada pautan-pautan mencurigakan yang diterima melalui e-mel serta sentiasa berwaspada dan berhati-hati dengan sebarang panggilan telefon atau mesej daripada mana-mana individu (sama ada yang dikenali atau tidak dikenali) yang meminta anda berkongsi kod khas seperti kod keselamatan (*'Security Code')* kepada akaun media sosial serta aplikasi pemesejan anda. Perkongsian kod khas tersebut hanya akan memberi peluang mudah kepada pihak tidak bertanggungjawab bagi mengambil alih akaun media sosial atau aplikasi pemesejan anda.

JABATAN KOMUNIKASI KORPORAT MCMC