BRI Buka Suara soal Penipuan Bermodus Undangan Nikah Digital via WA

28 Januari 2023

Jakarta – PT Bank Rakyat Indonesia (Persero) Tbk atau BRI buka suara atas maraknya penipuan dengan modus permintaan untuk meng- install aplikasi undangan pernikahan. Pihak BRI menjelaskan cara kerja pelaku adalah berpura-pura sebagai pihak pengirim undangan dengan mengirimkan file ekstensi apk, disertai foto undangan pernikahan kepada korban. Kemudian korban diminta untuk mengklik dan meng-install aplikasi tersebut. Selanjutnya, korban harus menyetujui hak akses (permission) terhadap beberapa aplikasi sehingga data pribadi yang bersifat rahasia dalam handphone korban bisa dicuri oleh pelaku.

Dijelaskan bahwa data yang dicuri sangat beragam, data yang bersifat pribadi dan berbagai informasi yang masuk melalui SMS, termasuk data perbankan yang bersifat rahasia seperti OTP (One Time Password) dan data lainnya dapat diambil oleh fraudster.

1. Nasabah diminta waspada Direktur Jaringan dan Layanan BRI Andrijanto mengimbau nasabah dan masyarakat lebih berhati-hati atas adanya kejahatan perbankan dengan modus mengirim undangan pernikahan tersebut. Diharapkan korban dari kejahatan perbankan tidak bertambah. "Nasabah agar selalu waspada terhadap berbagai modus tindak kejahatan social engineering. Kerahasiaan data pribadi dan data transaksi perbankan harus terus dijaga, tidak hanya oleh pihak bank, namun juga oleh nasabah," katanya dalam keterangan tertulis.

   BRI secara masif terus mengimbau nasabah agar lebih berhati-hati, serta tidak mengunduh, menginstal, maupun mengakses aplikasi tidak resmi. Nasabah juga diimbau meningkatkan kewaspadaan dengan tidak memberikan informasi data pribadi maupun data perbankan yang bersifat rahasia (seperti user id mobile banking, password, PIN, One Time Password/OTP dsb.) kepada pihak mana pun, termasuk yang mengatasnamakan BRI. "Apabila masyarakat sudah terlanjur meng-install aplikasi yang tidak dikenal

tersebut, maka diimbau untuk segera melakukan uninstall aplikasi yang tidak dikenal tersebut," tuturnya.

2. Segera hubungi pihak BRI Bank pelat merah itu mengimbau apabila nasabah mendapat notifikasi melalui SMS, surat elektronik atas transaksi yang tidak dilakukan, segera hubungi Contact BRI yang resmi di 14017/1500017. Nasabah juga diimbau untuk tidak mudah percaya kepada akun-akun social media tidak resmi yang mengatasnamakan BRI, adapun saluran komunikasi resmi BRI (centang biru/verified) hanya dapat diakses nasabah melalui www.bri.co.id, Instagram: @bankbri_id, Twitter: bankbri_id, kontak bri, promo_bri, Facebook: Bank BRI, YouTube: Bank BRI, TikTok: Bank BRI, dan Contact BRI 14017/1500017.

   Dia menjelaskan bahwa kejahatan perbankan dengan modus social engineering tersebut juga dapat terjadi di bank manapun. Oleh karenanya, untuk memerangi kejahatan perbankan tersebut, BRI proaktif berkoordinasi dengan pihak kepolisian untuk mengungkap dan menangkap berbagai tindakan kejahatan perbankan yang merugikan nasabah dan masyarakat secara umum.

3. Pengguna biasanya abaikan peringatan saat instal aplikasi Pengamat keamanan siber Alfons Tanujaya mengatakan sebenarnya pengguna akan mendapat peringatan berkali-kali ketika menginstal aplikasi dari luar Play Store. Pengguna diingatkan dampak yang muncul ketika aplikasi itu diinstal seperti memberikan akses SMS kepada aplikasi yang ingin diinstal, termasuk data dokumen dan foto perangkat kepada aplikasi.

   "Namun kemungkinan besar karena masyarakat tidak terbiasa memperhatikan peringatan ketika instal aplikasi dan dengan mudah memberikan persetujuan tanpa membaca dengan teliti dan mengerti akibat dari persetujuan yang diberikan, maka aplikasi jahat pencuri data ini akan tetap terinstal dan menjalankan aksinya," ujar Alfons dalam keterangannya.

Apabila data pengguna sudah bocor, Alfons menyarankan pengguna mengubah password dari berbagai aplikasi yang ada di handphone. Hal ini juga berlaku bagi pengguna mobile banking.

"Jika anda masih ragu, pertimbangkan untuk mengganti akun m-banking atau memilih penyedia m-banking yang memberikan pengamanan lebih baik," ujarnya.