KEMENTERIAN PENDIDIKAN, KEBUDAYAAN,
RISET, DAN TEKNOLOGI
POLITEKNIK NEGERI BANDUNG
Jln. Gegerkalong Hilir, Desa Ciwaruga, Kecamatan Parongpong,
Kabupaten Bandung Barat 40559, Kotak Pos 1234, Telepon: (022) 2013789
POLBAN Faksimile: (022) 2013889, Laman: www.polban.ac.id, Pos elektronik: polban@polban.ac.id

NOTA DINAS
Nomor B/7450/PL1/KP.15.00/2024

Yth. : Dosen ASN Polban
Dari : Direktur
Hal : Pencegahan Malware dan Keamanan Akun SISTER

Menindaklanjuti Hasil Sosialisasi Pencegahan Malware dan Keamanan Akun SISTER dari Tim Kemendikburistek, dengan ini disampaikan hal-hal sebagai berikut:

1. bahwa terdapat temuan akun SISTER yang terindikasi terkena malware disebabkan oleh kelalaian pengguna sehingga membutuhkan langkah peningkatan keamanan;
2. bahwa untuk menjaga keamanan akun SISTER, Bapak/Ibu dapat menerapkan beberapa hal sebagai berikut:
   a. pastikan untuk tidak membagikan akses akun SISTER kepada siapapun;
   b. gunakan password yang berbeda dengan password akun pada platform lainnya;
   c. gunakan password yang tidak mengandung informasi pribadi (contoh: nama, tanggal/bulan/tahun lahir, dsb);
   d. ubah/ganti password Akun SISTER secara berkala;
   e. menggunakan password manager untuk menyimpan password (contoh: 1password, google password manager, dsb);
   f. pastikan setiap platform website yang digunakan menggunakan protokol HTTPS untuk menghindari credentials sniffing;
   g. menghindari phising website dengan memastikan domain & URL yang dikunjungi adalah valid, seperti:
      1) https://sister.kemdikbud.go.id
      2) https://ssopddikti.kemdikbud.go.id/
      3) https://sso-pddikti.belajar.id/
      4) https://akses.kemdikbud.go.id/
   h. melakukan implementasi 2FA untuk semua akun yang digunakan (TOTP, email 2FA, SMS 2FA, dll), nantinya ini akan berlaku juga di platform SISTER.
3. bahwa untuk menghindari perangkat terinfeksi malware, berikut beberapa langkah yang dapat dilakukan:
   a. gunakan sistem operasi yang diupdate secara berkala (windows, linux, macos, android, ios, dll;
   b. gunakan antivirus terpercaya untuk mencegah eksekusi beberapa macam malware (Windows defender, Kaspersky, bitdefender, dll);
   c. gunakan Firewall pada konfigurasi sistem operasi;
   d. hindari instal browser extension dari untrusted source;
   e. hindari click link sembarangan saat beraktivitas di dalam internet;
   f. hindari instal software dari sumber yang tidak terpercaya (bajakan, cracked/mod version, aplikasi bukan dari play store/app store);
   g. lakukan backup data secara rutin di penyimpanan eksternal untuk tindakan preventif kehilangan data akibat malware.

Perlu kami sampaikan pula bahwa malware stealer dan ransomware adalah jenis malware yang mencuri data seperti kata sandi, informasi kartu kredit, dan data pribadi lainnya. Untuk itu, kami himbau seluruh dosen menjaga keamanan akun SISTER dengan melakukan pembaruan kata sandi secara berkala (3-6 bulan sekali) dan memastikan bahwa kata sandi baru yang Bapak/Ibu pilih berbeda dari yang sebelumnya.

Demikian kami sampaikan, atas perhatian Bapak/Ibu diucapkan terima kasih.

25 September 2024
Direktur,

Marwansyah, S.E., M.Si., Ph.D.
NIP 196405041990031002