BADAN SIBER DAN SANDI NEGARA

SERI BUKU SAKU

Persiapkan Keamanan Libur Lebaranmu

Dengan Tips & Trik
supaya liburanmu terhindar
dari ancaman siber

BADAN SIBER DAN SANDI NEGARA

Edisi
2025

www.bssn.go.id

#JagaRuangSiber

Hai, Sobat Siber!

Libur lebaran selalu menjadi momen yang dinantikan banyak orang. Selain waktu untuk berkumpul dengan keluarga, masa ini juga identik dengan meningkatnya aktivitas digital, seperti belanja *online*, transfer uang, hingga berbagi momen di media sosial. Tapi ternyata, di balik keseruan itu, ada banyak risiko keamanan informasi yang sering luput dari perhatian kita.

Kebahagiaan dan suasana liburan, sering kali membuat banyak orang yang terburu-buru melakukan transaksi tanpa berpikir panjang, mengklik tautan yang tidak jelas, dan juga menggunakan WiFi publik tanpa perlindungan. Hal ini bisa menjadi celah bagi penjahat untuk mencuri data pribadi, membobol rekening, atau menyebarkan *malware*. Modus penipuan pun semakin canggih, mulai dari *phishing* berkedok diskon Lebaran, SMS palsu tentang tiket mudik, hingga situs *e-commerce* abal-abal yang menawarkan harga murah untuk menipu pembeli.

Karena itu, penting bagi kita untuk lebih waspada dan memahami cara melindungi diri di dunia digital. Dengan mengetahui ancaman yang ada dan menerapkan langkah-langkah keamanan sederhana, kita bisa menikmati libur Lebaran dengan lebih tenang, tanpa takut jadi korban kejahatan siber. Libur lebaran nyaman, data harus tetap aman!

Selamat membaca dan menikmati liburan dengan tenang!

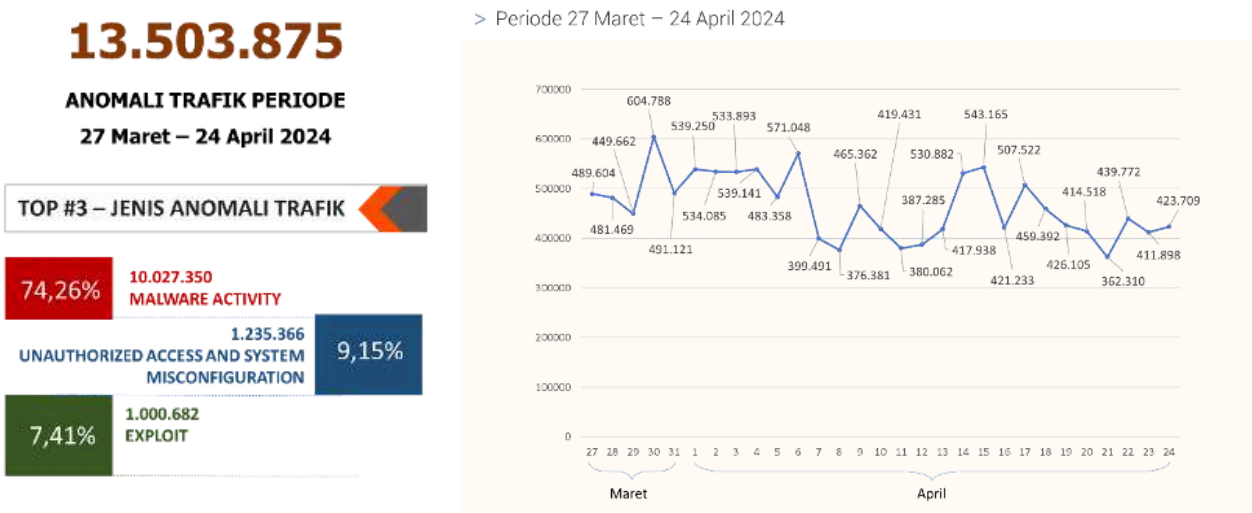
Daftar Isi

TERBIT
Maret 2025

LEBARAN BERKAH, TERNYATA JUGA BANYAK CELAH

Hari raya idul fitri selalu menjadi momen silaturahmi dan berkumpul dengan keluarga. Tapi ternyata, lebaran juga menjadi momen pelaku kejahatan siber untuk melancarkan semua modus penipuan melalui media digital. Phishing, penipuan online, dan pencurian identitas semakin marak dengan menggunakan modus diskon palsu, undian berhadiah, hingga investasi bodong.

Melihat kembali Ramadhan dan lebaran 2 tahun lalu, berdasarkan hasil deteksi yang dilakukan oleh BSSN periode 8 April s.d. 6 Mei 2023, terdapat lebih dari 25 juta anomali trafik di Indonesia. Bahkan, puncak anomali trafik ada di tanggal 18 April, 4 hari menjelang lebaran, yang mencapai lebih dari 1,6 juta. Hari-hari itu biasanya adalah momen orang-orang bersemangat membeli berbagai macam kebutuhan lebaran terlebih secara *online*. Selain itu, momen lebaran tahun 2023 juga dihebohkan dengan kasus penipuan QRIS palsu yang ditempelkan di kotak amal masjid agar donasi masuk ke rekening penipu. Ada juga modus kurir *e-commerce* palsu yang menjerat banyak korban dengan tautan berisi *malware* untuk mencuri data pribadi.



Bergerak maju ke lebaran tahun lalu, meskipun tidak setinggi sebelumnya, tapi anomali trafik juga mencapai angka yang tinggi di 4 hari dan bahkan 1 hari sebelum lebaran. *Malware* juga masih mendominasi jenis anomali yang seringkali diselipkan dalam tautan atau pesan singkat. Penipuan Salam Lebaran juga menjadi kejahatan siber yang populer di tahun ini. Modus yang menyebar lewat WhatsApp & SMS ini berisi tautan berbahaya yang bisa mencuri akun dan transaksi perbankan korban.

Hal ini menjadi bukti bahwa ternyata lebaran tidak luput dari kejahatan siber. Lalu bagaimana dengan lebaran tahun 2025? Teknik kejahatan siber yang semakin canggih seperti *phishing* berbasis AI dan deepfake tentunya memberikan ancaman yang lebih besar di hari raya ini. Jadi, jangan lengah! Mari lebih bijak dalam bertransaksi digital untuk melindungi diri dari serangan siber, agar momen penuh berkah ini tidak menjadi celah untuk para pelaku kejahatan siber.

PROMO MENARIK BUKAN BERARTI HARUS SELALU DIKLIK

Libur lebaran tentunya menjadi momen bagi semua orang untuk berkumpul bersama keluarga. Selain sebagai ajang berbagi kebahagiaan dan kemenangan, momentum ini juga menjadi ajang persaingan yang ketat bagi para penyedia untuk membagikan promo menarik seperti, tiket murah, diskon baju lebaran, sampai promo tempat wisata.

Berbagai cara menarik dilakukan untuk memikat konsumen. Tapi, tahukah kamu bahwa di balik euforia ini, penjahat siber juga ikut "berpromosi" lewat pesan WhatsApp atau email palsu. Ibarat udang dibalik batu, ada hal yang disisipkan oleh penipu untuk mendapatkan data pribadi yang bisa disalahgunakan dan tentunya akan sangat merugikan korban.

Ada kalanya kita tergoda dengan promo yang sangat meyakinkan, hingga tanpa berpikir panjang langsung membukanya. Kita terus mengikuti perintah yang diberikan seperti mengunduh *file* tertentu hingga menyetujui hak akses pada lokasi, kamera, dan *file* manager. Tapi ternyata, *file* yang diunduh tidak memunculkan data apapun dan hanya menampilkan *error* saja. Prank, bukan ? WhatsApp juga menjadi sarana untuk modus pengiriman *file* dengan ekstensi .apk yang meminta targetnya untuk menginstall *file* tersebut dengan dalih bagi-bagi promo dan kejutan. Yaa, memang terkejut! Bukan terkejut karena promo terbaik melainkan terkejut dengan *malware* yang menyerang perangkat target.

Nah untuk itu **PENTING** bagi kita untuk memastikan bahwa apa yang kita terima berasal dari pihak yang valid sebelum kita buka. Waspadalah! Karena bagaimanapun, keamanan dan informasi kita adalah tanggung jawab kita.

JARINGAN AMAN, MUDIK MENYENANGKAN

Saat libur lebaran, transportasi umum menjadi pilihan utama para pemudik. Saat ini, sebagian besar angkutan umum menyediakan akses Wi-Fi gratis untuk penumpangnya. Selain itu, area-area publik juga menyediakan Wi-Fi agar pemudik tetap nyaman saat perjalanan. Tapi, ada caranya lo supaya kita bisa tetap aman menggunakan Wi-Fi publik.

Pertama, pastikan jaringan WiFi yang digunakan adalah jaringan resmi. Utamakan untuk menggunakan jaringan yang disediakan oleh operator transportasi atau pihak resmi yang kredibel lainnya.

Kedua, hindari akses informasi pribadi atau sensitif, seperti nomor kartu kredit, kata sandi, atau informasi pribadi lainnya ketika menggunakan wifi. Oiya, jangan lupa untuk memastikan aplikasi antivirus yang kamu gunakan selalu *up to date* ya.

Ketiga, saat menggunakan Wi-Fi publik, hindari juga mengunduh atau membuka lampiran email atau pesan yang tidak dikenali. Jangan buka situs web yang mencurigakan atau asing, terutama yang meminta informasi pribadi atau rahasia.

Keempat, pastikan perangkat kita terkunci dengan kata sandi yang kuat dan jangan bagikan kata sandi dengan siapa pun. Awasi selalu perangkat kamu saat terhubung ke Wi-Fi publik, jangan tinggalkan tanpa pengawasan ya. *Last but not least*, pastikan kamu selalu mematikan Wi-Fi di perangkat setelah selesai menggunakannya, terutama saat meninggalkan area dengan jaringan Wi-Fi publik.

TRANSAKSI ONLINE MEMANG MEMUDAHKAN, TAPI...

Libur lebaran merupakan salah satu momen di mana angka transaksi online mencapai puncaknya. Tapi jangan sampai uang kita jatuh ke pihak yang salah ya. Nah berikut beberapa tips untuk memastikan transaksi kita benar dan tetap aman ya.

1. Pastikan hanya melakukan pembayaran kepada pihak yang sah dan tepercaya, seperti toko atau merchant resmi yang kita kenal dan percayai. Jangan mudah percaya jika penjual lebih mengarahkan transaksi melalui pesan singkat dibanding aplikasi toko *online* resmi.

2. Gunakan metode pembayaran yang aman, seperti QRIS atau transfer bank *online* melalui layanan yang resmi dan tepercaya.

3. Selalu periksa informasi transaksi dengan teliti sebelum melakukan pembayaran, termasuk jumlah pembayaran, kode QRIS atau nomor rekening tujuan, dan nama penerima. Jangan ragu untuk bertanya kepada pihak yang bersangkutan jika terdapat ketidakcocokan atau ketidakjelasan pada informasi transaksi.

4. Jika kamu curiga atau merasa ada indikasi penipuan, segera hubungi pihak terkait dan laporkan kejadian tersebut kepada pihak yang berwenang seperti polisi atau otoritas jasa keuangan.

5. Jangan memberikan informasi pribadi seperti nomor kartu kredit atau *password* kepada pihak yang tidak dikenal atau mencurigakan.

SARING SEBELUM SHARING,
BIAR GAK MALU DI GRUP CHATTING!

Informasi yang beredar tidak selamanya aktual apalagi faktual. Banyak sekali berita yang seliweran tanpa rujukan yang valid beredar di grup-grup Whatsapp. Dengan kata lain informasi itu bisa saja dibuat-buat atau direkayasa. Sebagai pengguna yang cerdas, kita harus dapat memastikan kebenaran informasi yang kita terima sebelum mempercayainya, menggunakannya sebagai referensi, atau bahkan menyebarkannya. Untuk memastikan kebenaran informasi yang diterima, kita bisa melakukan beberapa langkah berikut:

Verifikasi Sumber Informasi

Pastikan informasi yang kita terima berasal dari sumber yang terpercaya dengan reputasi yang baik. Cobalah untuk mencari sumber informasi lain yang berbeda dan bandingkan informasi yang diberikan.

Periksa Fakta

Lakukan pengecekan fakta dengan mencari informasi yang berkaitan dengan topik yang sama. Jangan hanya mengandalkan satu sumber informasi saja.

Gunakan Logika

Gunakan logika dan akal sehat untuk mengevaluasi informasi yang diterima. Apabila terdapat informasi yang terlalu mengada-ada, jangan langsung mempercayainya tanpa melakukan pengecekan lebih lanjut.

Perhatikan Konteks

Informasi yang diterima harus dilihat dalam konteks yang tepat. Perhatikan kembali apakah informasi yang diterima sesuai dengan waktu dan tempatnya.

Agar tidak terjebak *hoax*, penting bagi kita mengenali istilah dan jenis-jenis *hoax* yang sering beredar. *Hoax* bisa berupa berita palsu, judul sensasional (*clickbait*), konten palsu, konten tiruan, koneksi atau konteks yang salah, konten editan, hingga rumor dan teori konspirasi. Ada juga perbedaan antara disinformasi (sengaja menipu) dan misinformasi (salah karena ketidaktahuan).

Semoga kita semua dilindungi dari perbuatan keji seperti menyebar *hoax* ke orang terdekat dan terjebak *hoax* dari orang terkasih yaaa.

BATERAI PERANGKAT SELULER HABIS, LANGSUNG AJA AH KE STASIUN PENGISIAN DAYA

Ramainya pemudik di tempat umum seperti stasiun, bandara, pusat perbelanjaan, dan lain sebagainya menjadikan stasiun pengisian daya gratis menjadi salah satu tempat singgah favorit. Kegunaan perangkat seluler yang kini menjadi kebutuhan utama menjadikan pengisian daya menjadi prioritas. Stasiun pengisian daya USB memang merupakan fasilitas gratis yang dirancang untuk menyediakan beberapa port USB yang memungkinkan pengisian daya secara bersamaan untuk berbagai perangkat elektronik, seperti *smartphone*, tablet, *power bank, smartwatch*, dan perangkat lainnya yang mendukung pengisian melalui kabel USB. Tapi, apakah kamu yakin itu aman?

Seperti kata pepatah, “air tenang menghanyutkan” yang berarti bahwa sesuatu yang terlihat tenang atau tidak mencolok bisa jadi menyimpan hal yang perlu diwaspadai. Begitu juga dengan stasiun pengisian daya USB gratis ini. Mari kita mengenal *Juice Jacking*, pencurian data sensitif dari perangkat seluler lewat kabel USB yang terhubung.

Juice jacking adalah serangan *man-in-the-middle* yang berfokus pada perangkat keras. Penyerang menggunakan koneksi USB untuk memuat *malware* langsung ke stasiun pengisian daya atau menginfeksi kabel koneksi dan membiarkannya tetap terhubung, berharap orang yang tidak menaruh curiga datang dan menggunakan kabel yang "terlupakan".

Nah, oleh karena itu, supaya mudik dan liburan kita tetap aman, hindari penggunaan pengisi daya yang dibiarkan tersambung ke stopkontak sembarangan ya. Selain itu, selalu perbarui perangkat antivirus dan program perangkat lunak. Jangan pernah menerima perangkat pengisi daya promosi gratis atau perangkat dari sumber yang tidak terverifikasi ya.

SUDAH BERUSAHA MENJAGA, TAPI TETAP KENA SERANGAN? INI SOLUSINYA

Langkah pertama dan yang paling utama ketika terkena serangan siber adalah **Jangan Panik**. Identifikasi serangan apa yang sedang terjadi dengan tenang agar bisa melakukan langkah-langkah selanjutnya dengan bijak ya!

1. Jika terkena penipuan online (*phishing*, qris palsu, atau penipuan undian berhadiah), langsung blokir kontak penipu, cek mutasi rekening, dan laporkan ke bank atau layanan terkait untuk cegah kerugian lebih lanjut. Jangan lupa juga laporkan ke ke pihak berwenang dan sebarkan info ke orang terdekat agar mereka tidak ikut tertipu.

2. Jika terkena serangan *malware* atau virus dari *file* apk atau tautan berbahaya, segera putuskan koneksi internet, hapus aplikasi aneh, dan ganti semua kata sandi penting sambil aktifkan 2FA. Jangan lupa juga *scan* perangkat dengan antivirus dan laporkan ke pihak berwenang untuk penanganan lebih lanjut.

3. Jika akun media sosial atau perbankan diretas, langsung ganti *password*, aktifkan 2FA, dan laporkan ke *platform* terkait supaya akses bisa diamankan. Cek *login* mencurigakan, hubungi bank jika perlu, dan ingatkan keluarga supaya tidak jadi korban selanjutnya.

4. Jika mengalami kebocoran data pribadi, segera laporkan ke pihak terkait ya. Aktifkan keamanan tambahan dan hindari klik *link* dari pihak tak dikenal yang mengaku bisa bantu, bisa-bisa malah makin bahaya.

5. Jika terindikasi mengalami penipuan berkedok kurir *e-commerce* atau penerimaan paket, jangan klik tautan dalam pesan, abaikan dan cek langsung ke layanan resminya. Segera blokir dan laporkan nomor penipu untuk mencegah korban tertipu lainnya.

Setelah melakukan seluruh prosedur dengan benar, jangan lupa untuk berdoa dan bermuhasabah diri agar ke depannya bisa lebih waspada dan tidak mengulangi kesalahan yang sama ya!

Penutup

Di era digital yang semuanya saling terhubung, data adalah "emas baru". Di tangan yang tepat, data dapat menciptakan inovasi luar biasa, tetapi di tangan yang salah, data juga bisa menjadi senjata yang menghancurkan. Libur lebaran adalah momen yang seringkali digunakan oleh para pengincar data. Buku saku ini disusun sebagai pedoman dalam melindungi data kita selama libur lebaran.

Direktorat Operasi Keamanan Siber

BADAN SIBER DAN SANDI NEGARA Jalan Harsono R.M. Nomor 70, Ragunan, Pasar Minggu, Jakarta Selatan 12550 Telepon (021) 7805814, Faksimile (021) 78844104 Website : https://bssn.go.id, E-mail : humas@bssn.go.id

SERI BUKU SAKU

Persiapkan Libur Lebaran-mu

Dengan Tips & Trik supaya liburanmu terhindar dari ancaman siber

Edisi
2025

BADAN SIBER DAN SANDI NEGARA