

CARA AMAN BERTRANSAKSI

Untuk keamanan Anda dalam bertransaksi, harap diperhatikan beberapa hal sebagai berikut:

USER ID, PASSWORD, TOKEN

1. Gantilah Password J TRUST NET Individual & J TRUST MOBILE Anda secara berkala dengan kombinasi yang unik dan sulit diketahui oleh orang lain.
2. Jangan memberikan password atau PIN Anda ke pihak lain, termasuk ke petugas Bank.
3. Hindari menyimpan Password J TRUST NET Individual & J TRUST MOBILE di computer/Laptop, Smartphone dan Tablet Anda.
4. Jangan pernah mengirimkan informasi sensitif melalui email. Perlu diketahui bahwa J Trust Bank tidak akan meminta informasi sensitif melalui email atau sarana elektronik lainnya yang tidak aman.

PERANGKAT KOMPUTER/ LAPTOP, SMARTPHONE/TABLET

1. Gunakan komputer pribadi dan jaringan yang terpercaya untuk mengakses layanan J TRUST NET Individual & J TRUST MOBILE. Sebaiknya menghindari penggunaan komputer publik, misalnya di warnet, dan/atau jaringan yang tidak terpercaya, misalnya *wifi access point* yang disediakan oleh kafe atau toko di pusat perbelanjaan.
2. Selalu lakukan update/pengkinian versi *web browser* atau aplikasi yang Anda gunakan untuk bertransaksi melalui J TRUST NET Individual & J TRUST MOBILE.
3. Memastikan bahwa computer/ laptop yang digunakan aman dari perangkat *key logger*.

NETWORK/ JARINGAN

Jangan menggunakan akses *Wi-Fi* publik pada saat melakukan transaksi melalui J TRUST NET Individual & J TRUST MOBILE. Jaringan nirkabel yang tersedia untuk publik juga bisa dimanfaatkan oleh pelaku kejahatan untuk mencuri informasi dari ponsel, salah satunya informasi perbankan.

ZONA AMAN

Gunakan aplikasi resmi yang dikeluarkan khusus oleh J Trust Bank dengan mengunduh aplikasi J TRUST MOBILE langsung dari *application store* atau dengan mengakses situs resmi J Trust Bank. Atau untuk mengetahui berada dalam zona aman, mulailah dengan URL yang benar, seperti '*https*'. Juga bisa dengan melihat gambar gembok di bagian pojok kanan bawah layar monitor yang menunjukkan apakah *website* yang dimasuki aman atau tidak.

VERIFIKASI

Sebelum melakukan transaksi apapun, pastikan terlebih dahulu bahwa sedang mengakses J Trust Bank. Verifikasi informasi seperti nomor yang bisa dihubungi dan alamat jelas jika terjadi kesalahan. Periksakan pula ke bank lewat telepon tentang nomor rekening yang dituju, mulai dari alamat *website* hingga nomor rekening yang sah.

PEMBAHARUAN

Lakukan terus pembaruan aplikasi mobile banking, update versi terbaru secara manual atau dengan mengaktifkan fungsi *auto-update*. Selalu menggunakan aplikasi versi terbaru pada layanan J TRUST MOBILE.

LAINNYA

1. Beberapa hal yang perlu diperhatikan terkait dengan keamanan bertransaksi melalui J TRUST NET Individual & J TRUST MOBILE adalah sebagai berikut:

a. Phishing

Phishing adalah cara penipuan yang dilakukan oleh pihak tertentu dengan cara membuat situs web palsu yang sangat mirip dengan situs web resmi milik Bank dengan bertujuan untuk mendapatkan informasi rahasia milik nasabah seperti *User ID* dan *Password* yang dapat digunakan untuk merugikan Nasabah. Pengamanan terhadap phishing dapat dilakukan dengan beberapa cara sebagai berikut:

1. Pastikan Anda mengakses J TRUST NET *Individual* melalui alamat resmi situs di <https://www.jtrustnet.com> atau menggunakan link yang tersedia pada website www.jtrustbank.co.id, Selalu periksa kembali ejaan nama situs web, jangan sampai ada kesalahan ketik, termasuk penggunaan simbol.
2. Membuat *short cut* atau menyimpan alamat situs J TRUST NET *Individual* pada browser (*bookmark*) sehingga Anda dapat menggunakan *short cut* dan *bookmark* tersebut untuk meminimalkan kesalahan pengetikan alamat situs web J TRUST NET *Individual*.
3. Mewaspadaai upaya penipuan dari oknum yang mengatasnamakan sebagai petugas J Trust Bank melalui telepon, faks atau email yang menanyakan data pribadi termasuk PIN. Petugas J Trust Bank tidak akan meminta atau menanyakan Password atau nomor PIN Anda.
4. Jangan pernah memasukkan User ID dan Password pada suatu halaman web yang terbuka otomatis (pop up) dan/atau dari link/tautan yang mencurigakan seperti dari iklan-iklan/banner digital di situs web.

b. Virus

Virus adalah *software* komputer yang dibuat dengan tujuan-tujuan tertentu untuk merusak sistem operasi, aplikasi, dan data di komputer yang terinfeksi. Virus dapat menyebar melalui banyak media seperti email, CD, removable storage, program yang diunduh dari internet, jaringan, dan juga dari halaman situs web yang tidak aman. Beberapa contoh dampak dari infeksi virus adalah perangkat komputer menjadi tidak stabil dan sering 'hang' (macet), data terhapus, dan beberapa program aplikasi menjadi tidak dapat berfungsi dengan baik. Pengamanan terhadap virus dapat dilakukan dengan beberapa cara sebagai berikut:

1. Menggunakan anti virus terkini untuk mencegah terinfeksinya komputer Anda dengan virus, *malware*, *spyware* ataupun bentuk aplikasi-aplikasi lainnya yang dapat merugikan.
2. Berhati-hati mengunduh *attachment* email karena dapat berisi virus yang dapat mencuri data sensitif. Lakukan *scan* atas *attachment* terlebih dahulu menggunakan software anti virus yang dimiliki sebelum dibuka.
3. Berhati-hati dalam mengunduh dan/atau menginstal *software*.
4. Berhati-hati dalam menghubungkan perangkat *removable storage* ke perangkat komputer Anda. Lakukan *scan* pada *removable storage* menggunakan *software* anti virus terlebih dahulu sebelum membuka isinya.
5. Menghindari akses ke dan/atau mengunduh file dari alamat *web* yang tidak terpercaya.

c. Spyware

Spyware adalah *software* komputer yang dibuat untuk mengambil informasi penting/pribadi seperti nomor kartu kredit, User ID dan PIN/Password, nomor rekening, alamat email, dan lain-lain dari perangkat komputer yang terinfeksi dan akan mengirimkan informasi tersebut ke lokasi tertentu untuk kepentingan pihak yang tidak bertanggungjawab. *Spyware* dapat ter-install melalui *attachment* email, program yang di-install dari sumber-sumber/situs web yang tidak aman. Virus juga dapat diprogram untuk menyebarkan *spyware*. Cara kerja *Spyware* cenderung sulit terdeteksi sehingga lebih mudah mengumpulkan informasi yang diinginkan pembuat/penyebarnya. Pengamanan terhadap *spyware* sama dengan pengamanan terhadap virus.

2. Untuk memastikan rincian sertifikat keamanan dan alamat situs web <https://www.jtrustnet.com/>, pilih View Certificate pada green bar/icon security di samping alamat web pada peramban yang Anda gunakan. Jika keluar pesan warning mengenai sertifikat saat mengakses J TRUST NET *Individual*, mohon Anda tidak mengakses situs web tersebut atau mengecek ulang nama situs web yang telah diketik.

3. Pastikan pada peramban Internet Anda terdapat gambar gembok/kunci yang mengindikasikan bahwa halaman yang Anda akses saat ini dienkripsi dengan menggunakan *Security Socket Layer (SSL)*. Jika Anda tidak melihat gambar gembok/kunci, dimohon Anda untuk melakukan Logout.
4. Jangan pernah melakukan pendaftaran J TRUST NET Individual untuk mendapatkan hadiah atau untuk alasan apa pun atas permintaan seseorang melalui telepon atau dengan cara lain. Lakukan pendaftaran layanan Elektronik Banking J Trust Bank secara resmi hanya melalui Kantor Cabang atau Portal Elektronik Banking J Trust Bank.
5. Apabila terdapat notifikasi dari J Trust Bank mengenai adanya aktivitas pada rekening sementara Anda tidak pernah melakukan hal tersebut, segera tindaklanjuti dengan mendatangi Kantor Cabang J Trust Bank terdekat atau call center J Trust Bank
6. Mengkonfirmasi kepada pihak J Trust Bank melalui call center J Trust "Ask J" di 1500615 jika ada permintaan yang mencurigakan.
7. Menghentikan aktivitas transaksi jika merasa ada yang ganjil/tidak biasa pada perangkat computer/laptop atau smartphone/tablet atau halaman web/ aplikasi yang sedang diakses.