KEAMANAN SELULER

PENGETAHUAN & SARAN PRAKTIK YANG BAIK

BNP PARIBAS

The bank for a changing world

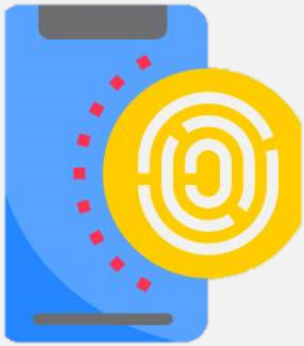
version control 0725-01

BNP Paribas memberikan beberapa tips dan praktik terbaik untuk membantu Anda menjaga perangkat seluler Anda seaman mungkin

Perlindungan Selular

Perlindungan Akses

- **Pertimbangkan untuk menggunakan kunci layar** sebagai langkah keamanan pertama guna melindungi perangkat seluler
- **Konfigurasikan kunci ponsel otomatis** setelah 5 menit tidak aktif
- **Jangan tinggalkan ponsel tanpa pengawasan**. Akses sementara ke ponsel mungkin cukup untuk dibobol tanpa sepengetahuan pengguna bahkan ketika terkunci
- **Batasi jumlah percobaan membuka kunci**, lalu atur waktu penguncian yang lebih lama serta penghapusan otomatis setelah belasan percobaan gagal
- **Kunci layar memang berguna**, tetapi tidak dapat mencegah seseorang mengeluarkan kartu SIM dari ponsel dan menggunakannya di ponsel lain
- **Untuk mengantisipasi risiko ini**, pengaturan kunci kartu SIM berupa nomor PIN harus dimasukkan pada saat ponsel dihidupkan agar dapat terhubung ke jaringan
- **Jangan hubungkan perangkat ke stasiun kerja yang tidak terkontrol atau perangkat lain yang tidak tepercaya**. Hal ini akan menyebabkan koneksi langsung yang tidak terkontrol



Pelacak Jarak Jauh

- **Pelacakan jarak jauh dapat diaktifkan jika ponsel hilang**
- **Nonaktifkan ponsel jika perlu** dengan menggunakan fungsi '**Temukan Perangkat Saya**' di Android atau '**Temukan iPhone Saya**' di Apple iPhone

Keamanan Aplikasi

- Aplikasi harus memiliki izin yang memadai untuk fungsinya, baik untuk akses data maupun internet, tetapi juga untuk kontrol berbagai sensor. Izin yang diberikan harus diperiksa setidaknya selama instalasi dan setiap pembaruan untuk memastikan bahwa izin tersebut belum diubah
- Aplikasi harus diperbarui secara berkala dan cepat karena *patch* keamanan ditawarkan

Akses Jaringan

Penggunaan Wi-Fi

- **Gunakan hanya jaringan Wi-Fi atau penyedia layanan tepercaya**
- **Selalu gunakan perlindungan keamanan** seperti *Wi-Fi Protected Access* (WPA), jika memungkinkan
- **Selalu matikan koneksi nirkabel Anda saat tidak digunakan**. Ini memastikan bahwa seseorang tidak dapat terhubung ke perangkat tanpa sepengetahuan dan kendali Anda. Sebaiknya periksa juga pengaturan keamanan jaringan ponsel Anda karena mungkin dikonfigurasi untuk terhubung secara otomatis ke jaringan saat berada dalam jangkauan tanpa sepengetahuan Anda
- **Pastikan *router* nirkabel kediaman Anda dilindungi oleh kode sandi**
- Jika Anda menggunakan seluler nirkabel atau *hotspot*, berhati-hatilah terhadap koneksi berbahaya yang terlihat sangat mirip dengan *hotspot* resmi dari perusahaan besar
- Untuk tindakan yang rahasia, sebaiknya gunakan koneksi 3G atau 4G, yang jauh lebih aman

Bluetooth

- ***Bluetooth*** umumnya tidak dianggap berisiko karena jangkauannya yang relatif lebih pendek (sekitar 10 meter). Namun, peretas diketahui dapat mengakses ponsel dari jarak jauh jika mereka berada dalam jangkauan
- Pastikan *Bluetooth* Anda dimatikan saat tidak digunakan. Konfigurasikan Bluetooth ke 'tidak dapat ditemukan', agar orang yang mencari perangkat di sekitar tidak dapat menemukan perangkat Anda
- Permintaan tidak dikenal yang muncul melalui koneksi *Bluetooth*, seperti tawaran untuk "pasangkan dengan perangkat" harus diabaikan atau ditolak. Peretas yang berada dalam jangkauan dapat menggunakan perangkat Anda melalui *Bluetooth*, jika tidak diamankan.

Akses VPN

- **Jaringan Pribadi Virtual** (VPN) adalah perangkat lunak yang dapat menutupi lokasi perangkat atau masuk ke situs web seolah-olah perangkat tersebut berada di negara lain
- VPN gratis berbahaya karena berbagai alasan:
  - *Malware* dapat disembunyikan dan mencuri data. Ini juga dapat digunakan untuk membajak akun dan mencuri uang
  - VPN juga dapat **membajak** peramban web dengan mengalihkan ke situs berbahaya lainnya tanpa izin
- Oleh karena itu, VPN harus digunakan dengan hati-hati dan biasanya lebih baik menggunakan penyedia VPN yang terkenal dan bereputasi baik serta membayar mereka. Meskipun jika berbayar, hal itu tidak menjamin keamanan

Akses Jaringan

Geolokasi

- Banyak aplikasi jejaring sosial ponsel pintar secara otomatis mengunggah foto ke internet karena banyak ponsel yang menyematkan tag lokasi, juga disebut ***'geotag'***, langsung ke dalam berkas foto
- Siapa pun yang memiliki perangkat lunak yang tepat dapat melihat foto-foto Facebook atau Flickr dan mengetahui di mana orang-orang telah berada dan berada saat itu
- Akses ke layanan geolokasi harus dilarang untuk aplikasi yang fungsi posisi geografisnya tidak digunakan. Jika opsi ini tidak tersedia dalam pertanyaan terminal, layanan geolokasi harus dinonaktifkan saat tidak digunakan

Pembaruan Sistem Operasi

- **Merek-merek ponsel pintar secara berkala melakukan penyempurnaan dan perubahan pada perangkat lunak seluler mereka**. Ini bukan hanya untuk menambahkan fungsi baru, tetapi juga pembaruan ini sering kali berisi perbaikan keamanan penting yang melindungi data dan perangkat dari peretas
- **Setiap perangkat yang tidak lagi mendukung evolusi sistem operasi harus diganti**

Proteksi Data

Perlindungan Data

- Merupakan keputusan yang bijaksana untuk meminimalkan informasi yang tersimpan di perangkat seluler karena perangkat jenis ini mudah hilang. Pilihan menggunakan hard disk eksternal untuk menyimpan informasi lebih aman.
- **Saat perangkat seluler harus diperbaiki, penting untuk mengeluarkan kartu memori sebelum memberikan perangkat seluler tersebut**
- Setiap pertukaran informasi sensitif harus dilakukan dalam bentuk terenkripsi untuk memastikan privasi dan integritas data titik-ke-titik.

Antivirus

- Kemampuan ponsel pintar mendekati kemampuan PC, tetapi kebanyakan orang tidak memiliki bentuk perlindungan, meskipun mereka dapat menghadapi ancaman serupa
- ***Spam* yang berisi lampiran malware atau tautan untuk menyerang situs atau aplikasi terinfeksi yang mengeksploitasi kelemahan sistem operasi mulai bermunculan**
- Banyak perusahaan antivirus kini menawarkan versi gratis untuk produk seluler komersial mereka dan juga perlindungan untuk beberapa PC dan ponsel dengan langganan tahunan
- Sayangnya, perangkat lunak antivirus palsu dirancang untuk menginfeksi perangkat atau membuat orang berpikir perangkat tersebut terlindungi sebenarnya tidak memberikan perlindungan yang lengkap

Penafian

Isi dari dokumen ini bersifat umum dan bukan merupakan nasihat hukum, keuangan, pajak atau profesional. Meskipun informasi yang dimuat dalam dokumen ini telah diperoleh dari sumber-sumber yang diyakini PT Bank BNP Paribas Indonesia dapat diandalkan, tidak ada pernyataan atau jaminan apa pun, tegas maupun tersirat, yang dibuat dan tidak ada tanggung jawab apa pun yang diterima atau akan diterima oleh PT Bank BNP Paribas Indonesia mengenai atau dalam kaitannya dengan keakuratan, keandalan atau kelengkapan dari informasi tersebut. Semua dan setiap tanggung jawab dan kewajiban tersebut secara tegas dan sepenuhnya disangkal.

Pendapat-pendapat yang dinyatakan dalam dokumen ini mencerminkan penilaian PT Bank BNP Paribas Indonesia pada tanggal dokumen ini dan dapat tunduk pada perubahan tanpa pemberitahuan apabila PT Bank BNP Paribas Indonesia mengetahui informasi apa pun, yang bersifat khusus ataupun umum, yang mungkin memiliki dampak material terhadap pendapat-pendapat tersebut.

Baik PT Bank BNP Paribas Indonesia maupun setiap afiliasinya atau direktur, pejabat atau karyawan masing-masing tidak bertanggung jawab atas setiap kerugian atau kerusakan yang diderita atau dialami oleh pihak mana pun akibat mengandalkan atau menggunakan dokumen ini.

Tidak ada hal apa pun dalam dokumen ini yang akan ditafsirkan sebagai pemberian atau penyerahan hak apa pun melalui lisensi atau sehubungan dengan setiap paten, hak cipta, merek dagang atau logo Grup BNP Paribas (termasuk pengetahuan teknis dan rahasia dagang) atau hak kekayaan intelektual lainnya.

Dokumen ini tidak dapat diproduksi kembali (secara keseluruhan maupun sebagian) dan tidak dapat diringkas atau didistribusikan tanpa persetujuan tertulis sebelumnya dari PT Bank BNP Paribas Indonesia.

PT Bank BNP Paribas Indonesia diatur dan diawasi oleh Otoritas Jasa Keuangan sebagai bank umum. Informasi dalam dokumen ini tidak dimaksudkan untuk didistribusikan kepada, atau digunakan oleh, atau bukan merupakan penawaran apa pun kepada, setiap orang atau badan di yurisdiksi manapun apabila (a) pendistribusian atau penggunaan atau penawaran informasi tersebut akan bertentangan dengan hukum atau peraturan, atau (b) PT Bank BNP Paribas Indonesia akan menjadi tunduk pada persyaratan hukum atau peraturan yang berlaku.

Dengan menerima dokumen ini, Anda sepakat untuk terikat pada pembatasan-pembatasan tersebut di atas.