SAMSUNG

SIARAN PERS

Begini Cara Samsung Lindungi Smartphone-mu dari Serangan Siber

**gambar untuk ilustrasi*

Jakarta, 19 November 2021 - Smartphone telah menjadi benda penting yang menemani kita bekerja, hidup, hingga bermain. Bagi sebagian orang, smartphone bahkan menjadi satu-satunya barang yang kita bawa keluar rumah, menggantikan laptop hingga dompet.

Meskipun saat ini kebanyakan orang telah sadar akan bahaya yang dimunculkan peretas (*hacker*) terhadap laptop dan komputer, kita juga perlu menyadari bahwa smartphone juga rentan terhadap serangan siber. Peretas mengincar benda yang sedang banyak digunakan dan saat ini, benda tersebut adalah perangkat seluler. Itulah mengapa menjaga keamanan smartphone menjadi lebih penting, dan Samsung pun terus berinovasi untuk melindungi konsumen dan data konsumen dari ancaman yang muncul.

Miliaran smartphone di seluruh dunia saat ini dipenuhi dengan data pribadi dan data bisnis yang sensitif, memberikan peluang tak terbatas bagi para peretas untuk mencuri dan menjual informasi pribadi tersebut. Faktanya, perusahaan keamanan siber, IronNet, melaporkan bahwa serangan siber telah meningkat sebanyak 168% antara Mei 2020 dan Mei 2021, dan serangan terhadap smartphone menjadi salah satu ancaman keamanan siber terbesar di kawasan Asia Pasifik.

Samsung berkomitmen untuk menjaga pengguna agar tetap aman dan terlindungi, dengan **Samsung Knox** memberikan perlindungan menyeluruh di seluruh siklus hidup perangkat Anda. Berikut lima skenario potensi serangan siber yang dapat terjadi ketika keamanan perangkat Anda terganggu – dan bagaimana Samsung Knox melindungi Anda dari ancaman ini, sejalan dengan etos kami dalam menempatkan keamanan konsumen sebagai prioritas.

Skenario 1 Serangan Siber: Akses *backdoor* tanpa persetujuan

Di luar Samsung, pengembang secara rutin membuat *backdoor* atau 'pintu rahasia' untuk aplikasi dan bahkan sistem operasi (OS) seluler sehingga mereka dapat memperoleh akses yang mudah saat perlu melakukan *troubleshooting*. Namun, peretas dapat menemukan *backdoor* ini, yang biasanya melompati satu atau semua pengaman siber pada perangkat yang dimaksud.

Untuk mencegah akses *backdoor* tanpa persetujuan, jangan mengunduh aplikasi tidak resmi atau tidak sah. Mengunduh perangkat lunak selain yang dipasang pabrikan sejak awal untuk mendapatkan akses penuh ke sistem operasi perangkat juga dapat mengundang malware atau spyware yang mengarah ke akses *backdoor* tanpa persetujuan.

Di Samsung, kami merancang, membuat, dan memvalidasi setiap chip komputer, setiap kabel, dan setiap komponen perangkat keras sebelum menggunakannya untuk memproduksi perangkat pintar kami di pabrik yang sangat aman di seluruh dunia. Pendekatan ini memberi kami kendali atas desain, manufaktur, dan perakitan, memastikan rantai pasokan aman yang mencegah akses *backdoor* tanpa persetujuan di perangkat kami – menghasilkan produk yang dapat dipercaya sepenuhnya oleh konsumen.

Skenario 2 Serangan Cyber: Password yang bocor, lemah, atau dipakai ulang

Seiring perkembangan jaman, kita terus membuat akun baru untuk berbagai layanan digital, mulai dari layanan konsultasi dokter online, platform transportasi online hingga *e-commerce* baru. Tanpa disadari hal ini menyediakan lebih banyak jalan untuk dieksploitasi oleh peretas.

Seperti yang ditemukan oleh IBM[1] di survei Agustus 2021, 86% konsumen di Asia Pasifik mengakui bahwa mereka menggunakan kembali password yang sama di beberapa akun online. Hal ini merupakan sebuah kebiasaan privasi data yang buruk – dimana satu serangan saja dapat membuat seluruh jejak internet pengguna rentan disalahgunakan peretas.

Perangkat Samsung [2] dilengkapi dengan teknologi otentikasi biometrik yang inovatif, seperti **Ultrasonic Fingerprint**, sehingga akses ke data Anda dapat dilindungi meskipun perangkat Anda hilang atau dicuri. Dikenal sebagai **Samsung Pass** [3], alat otentikasi biometrik ini juga memungkinkan pengguna dengan mudah mengakses kredensial masuk tanpa perlu mengingat nama pengguna dan kata sandi yang tak terhitung jumlahnya[4]! Untuk meningkatkan perlindungan data, Samsung juga telah melengkapi perangkat dengan **Knox Vault**, prosesor aman yang beroperasi secara independen dari CPU utama. Knox Vault mengisolasi data biometrik Anda dengan aman dari bagian lain ponsel Anda, sehingga tidak ada yang bisa mendapatkan data Anda.

Skenario 3 Serangan Siber: Wi-Fi gratis yang ternyata tidak sepenuhnya gratis

Hotspot Wi-Fi gratis adalah anugerah bagi semua orang yang membutuhkan akses Internet di perangkat seluler mereka untuk bekerja atau bermain. Namun, layanan Wi-Fi publik memberikan peluang bagi peretas untuk mencuri data, karena data yang Anda kirim melalui web – seperti informasi kartu kredit saat melakukan pembelian online – mungkin jatuh ke tangan peretas melalui jaringan Wi-Fi publik.

---

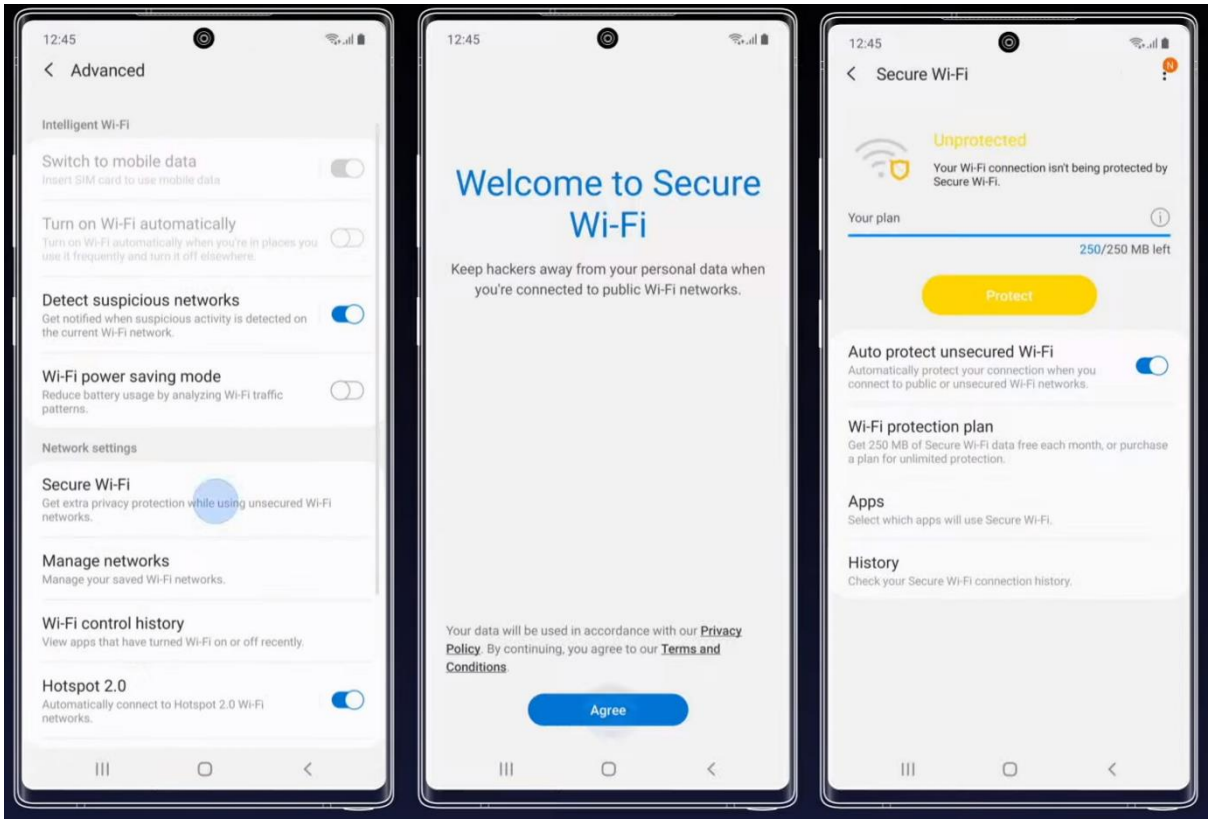
[1] IBM Security: Survei Konsumen IBM: Efek Samping Keamanan dari Pandemi: https://filecache.mediaroom.com/mr5mr_ibmnews/191177/Pandemic%20Security%20Side%20Effects%20Global%20Survey_IBM%20Analysis.pdf

[2] Ketersediaan fitur otentikasi biometrik dapat bervariasi menurut perangkat

[3] Fungsi, fitur, dan aplikasi yang kompatibel untuk Samsung Pass yang tersedia dapat berbeda di setiap negara karena lingkungan peraturan dan hukum yang berbeda.

[4] Untuk pengamanan terbaik, konsumen tetap disarankan untuk memasukkan password yang rumit untuk mengamankan kredensial login mereka.

Untuk *browsing* sehari-hari, Secure Wi-Fi[5] di perangkat Samsung mengenkripsi lalu lintas internet keluar dan menonaktifkan pelacakan pada aplikasi dan situs web. Hal ini memungkinkan Anda untuk menjelajah internet dengan aman pada Wi-Fi publik tanpa takut akan pelanggaran keamanan[6].



Skenario 4 Serangan Siber: Serangan *phishing* yang mengambil data sensitif

Phishing adalah jenis serangan di mana penjahat siber mengelabui korbannya untuk menyerahkan informasi sensitif atau memasang malware[7], menyamar sebagai tautan, lampiran, atau bahkan aplikasi yang sah, di perangkat mereka.

Setelah peretas memiliki akses ke informasi sensitif Anda, mereka dapat menggunakannya untuk meminta tebusan dari Anda, mencuri informasi pribadi Anda, melakukan kejahatan lain, bahkan melakukan pembelian dengan informasi kartu kredit Anda.

Samsung melindungi Anda dari ancaman ini lewat Device Protection di **Samsung Device Care** yang terus-menerus memindai perangkat Anda dari malware atau aktivitas mencurigakan dan memperingatkan Anda saat Anda salah memasang aplikasi berbahaya melalui deteksi melalui perlindungan McAfee.

---

[5] Ketersediaan Secure Wi-Fi dapat bervariasi tergantung pada negara, operator, atau lingkungan jaringan dan mungkin tidak didukung di semua perangkat seluler Samsung. Biaya mungkin berlaku tergantung pada penggunaan Secure Wi-Fi.

[6] Sebagai pengamanan terbaik, hindari menghubungkan perangkat ke hotspot Wi-Fi yang tidak dikenal dan selalu jaga keamanan jaringan Wi-Fi di rumah dengan password yang rumit dan panjang.

[7] https://www.itgovernance.co.uk/phishing

Selain itu, Samsung Secure Folder menjaga keamanan data dan mengisolasi aplikasi bermasalah di dalam folder untuk menjauhkan aplikasi dari informasi pribadi pengguna.

Skenario 5 Serangan Siber: Kerentanan *zero-day*

Mengingat peretas dan penyerang siber terus-menerus mencoba meretas perangkat, mereka selalu waspada terhadap kerentanan zero-day. Kerentanan zero-day adalah kerentanan dalam sistem atau perangkat yang telah ditemukan tetapi belum ditambal. Ini bisa sangat berbahaya karena penjahat dunia maya menargetkan kelemahan dalam sistem sebelum pengembang atau publik menyadarinya.

Samsung Knox menawarkan perlindungan secara *real time*, selalu secara aktif melindungi perangkat Anda dari serangan data atau malware. Ini berarti bahwa upaya tidak sah untuk mengakses atau memodifikasi ponsel Anda diblokir secara real time.

Saat pengguna melakukan *reboot* pada smartphone Samsung mereka, **Secure Boot** diaktifkan untuk mendeteksi perangkat lunak yang tidak sah dan memblokir upaya untuk menyusupi perangkat melalui

keamanan berlapis tingkat militer[8]. Jika smartphone di-*boot* dalam keadaan tidak disetujui, Samsung Knox akan secara otomatis mengunci aplikasi yang berisi data sensitif seperti Samsung Pass, Secure Folder, atau Samsung Health.

Mencapai masa depan yang lebih aman

Smartphone telah menjadi bagian penting dari kehidupan digital kita, baik dari rumah, di kelas, atau bahkan di kantor. Dengan berbagai ancaman baru bermunculan di dunia maya yang semakin berisiko, kita harus tetap waspada dan berperan aktif dalam menjaga keamanan diri kita dan orang yang kita cintai di dunia digital ini.

Keamanan tidak hanya disajikan dalam smartphone Samsung, karena perlindungan Knox juga meluas ke peralatan pintar dalam portofolio Samsung lainnya untuk lapisan perlindungan tambahan. Hal tersebut berarti elektronik rumah tangga pintar Samsung Anda dilindungi dan dijaga, baik saat Anda *mirroring* video yang Anda tonton di perangkat Galaxy Anda dengan aplikasi SmartView[9] ke layar televisi, atau saat menggunakan fungsi AI pada mesin cuci Samsung AI EcoBubble Anda untuk mengkalibrasi pengaturan pencucian yang optimal.

Para pengguna Samsung dapat yakin bahwa Anda memiliki mitra digital yang berkomitmen pada standar keamanan dan privasi kelas dunia – menjaga Anda tetap aman saat bekerja, belajar, maupun bermain.

-Selesai-

Tentang Samsung Electronics Co., Ltd.

Samsung Electronics Co., Ltd menginspirasi dunia dan membentuk masa depan dengan ide-ide dan teknologi transformatif. Perusahaan ini mendefinisikan ulang dunia televisi, ponsel pintar, perangkat wearable, tablet, peralatan digital, sistem jaringan, dan memory, sistem LSI, foundry dan solusi LED. Untuk berita terbaru, silakan mengunjungi Samsung Newsroom: http://news.samsung.com.

Untuk keterangan lebih lanjut hubungi:
Jane Tjondro
Public Relations Professional
PT Samsung Electronics Indonesia
Phone: 021-29588000
Email: j.tjondro@samsung.com

[8] Knox menerima lebih banyak akreditasi daripada produsen perangkat seluler lainnya, termasuk persetujuan STIG dari Badan Sistem Informasi Pertahanan AS untuk digunakan dalam jaringan DoD pada tahun 2013 dan sertifikasi dari Departemen Pertahanan AS, NCSC Inggris, dan ANSSI di Prancis.

[9] Kompatibel dengan semua aplikasi utama pada model Samsung Galaxy S6 atau perangkat yang lebih baru, menjalankan Android 8.1 atau lebih tinggi.