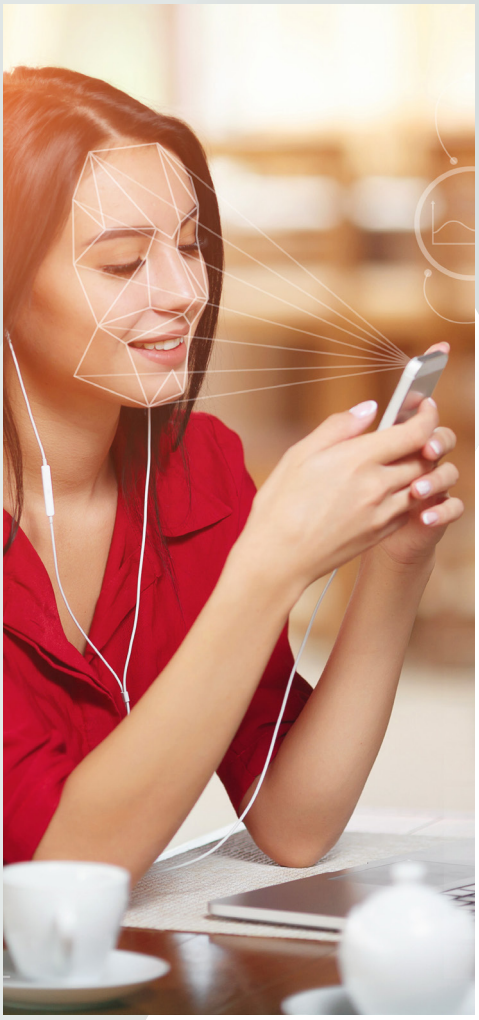
www.airome.tech

AIROME



PEMBUKTIAN KEASLIAN BIOMETRIK

Melindungi titik paling rentan pada saluran digital

Saat ini, pelaku kejahatan di dunia maya terus-menerus meningkatkan teknologi miliknya untuk mencuri uang dari akun pengguna saluran perbankan digital: serangan teknis, rekayasa sosial, atau gabungan keduanya ikut berperan. Ini menyebabkan kerugian finansial bagi bank dan pelanggan mereka, atau, paling tidak, membuat aksesibilitas pelanggan jauh lebih rumit.

Kecuali jika Anda ingin menerima panggilan dari spesialis anti-penipuan yang kadang membuat frustrasi atau mengundang pelanggan ke kantor untuk setiap perubahan kecil, cara paling inovatif untuk memperkuat keamanan pelanggan saluran perbankan digital adalah biometrik.

TUJUAN BISNIS

Membangun saluran digital yang memberi pelanggan kenyamanan dan ketenangan bahwa dana mereka aman, bukanlah pencapaian kecil. Penipu cenderung menyerang titik terlemah dalam sistem keamanan, biasanya pengguna akhir itu sendiri. Ini berarti kode rahasia atau kata sandi yang dikirim melalui SMS atau push-notification tidak efektif - penyerang dapat dengan mudah mempelajarinya dengan berpura-pura menjadi petugas keamanan.

Dalam hal keamanan, kasus paling sensitif adalah ketika pelanggan beralih ke perangkat seluler baru atau mencoba memulihkan akses ke akun pribadinya. Tanpa kontak fisik dengan pengguna, sulit bagi keamanan untuk mengidentifikasi siapa sebenarnya yang melakukan transaksi. Apakah pelanggan asli atau penipu yang berhasil mendapatkan semua informasi yang diperlukan dan memperoleh akses tanpa izin?

Untuk menghilangkan titik lemah dalam sistem keamanan, pertama-tama Anda harus berhenti mengandalkan kata sandi sekali pakai yang dikirimkan ke pelanggan melalui saluran yang tidak aman. Setelah itu, Anda harus menambahkan setidaknya satu faktor otentikasi lagi untuk transaksi penting.

Masalah keamanan layanan perbankan jarak jauh atau Remote banking services (RBS):

- Tingkat keamanan RBS tidak mencukupi saat pengguna menghubungkan dan memperbarui kunci penandatanganan mereka.
- Aktivitas penipuan perbankan tingkat tinggi, termasuk malware dan manipulasi psikologis.
- Otorisasi transaksi yang ketinggalan zaman dan tidak aman serta teknologi penandatanganan dokumen yang menggunakan SMS dan push-notification.

Platform PayConfirm dengan modul identifikasi biometrik memungkinkan Anda menggunakan faktor otentikasi biometrik tambahan saat pelanggan melakukan tindakan penting, seperti memperbarui kunci mereka atau menghubungkan perangkat seluler baru, atau saat mereka melakukan transaksi besar.

HASIL

Keuntungan dari solusi komprehensif:

- Menurunkan volume pencurian dari rekening pelanggan beberapa kali lipat.
- Pengalaman pengguna yang disederhanakan dalam hal memulihkan akses atau melakukan transaksi yang tidak biasa.
- Secara signifikan mengurangi beban pada spesialis anti penipuan dan pusat panggilan bank.
- Mengurangi biaya layanan telekomunikasi karena kode SMS.

HUBUNGI KAMI

airome.tech
info@airome.tech

Salah satu persyaratan utama bagi sistem agar dapat memecahkan masalah ini adalah memastikan kepenulisan dan integritas dokumen yang ditandatangani. Hal lainnya adalah memberikan faktor otentikasi biometrik tambahan.

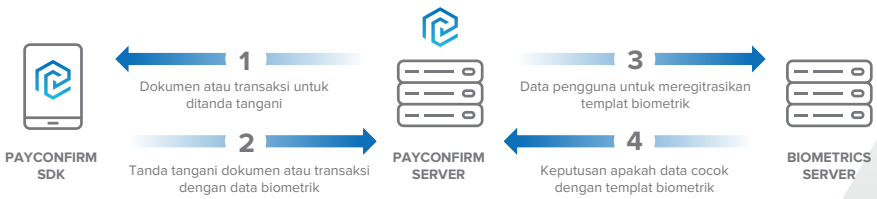
DESKRIPSI SOLUSI

PayConfirm, platform perangkat lunak dengan mobile transaction authentication signature atau tanda tangan otentikasi transaksi seluler (mTAS), adalah solusi terbaik yang memenuhi persyaratan ini, dengan menyertakan modul identifikasi biometrik dan perlindungan pada penipuan digital.

PayConfirm menggunakan teknologi tanda tangan digital seluler, yang memungkinkan Anda mengonfirmasi transaksi apa pun melalui saluran digital dengan satu ketukan layar, sambil memastikan kepemilikan dan integritasnya. Mode operasi ini tidak memaksa Anda untuk mengirim kata sandi satu kali ke pelanggan, yang berarti mereka tidak akan disadap atau disusupi. Mengintegrasikan dengan platform identifikasi biometrik akan memberikan keamanan tambahan untuk kasus yang paling rentan, seperti memulihkan akses pada perangkat baru.

CARA KERJA

Saat pengguna terhubung ke sistem, mereka mengambil gambar wajah mereka (selfie). Templat biometrik ini kemudian disimpan dalam database di sisi bank. Saat mencoba memulihkan akses di perangkat baru, pengguna akan diminta untuk mengambil foto selfie bersama dengan data yang biasanya diminta untuk disediakan (nomor kartu, kode SMS, dll.). Selfie ini kemudian dibandingkan dengan templat biometrik yang terdaftar untuk memverifikasi kegiatan mereka. Jika foto cocok dengan templat, akses akan dipulihkan, jika tidak maka tidak akan bisa.



Kerangka kerja yang sama dapat digunakan untuk mengotorisasi transaksi berisiko tinggi yang terdeteksi oleh sistem anti-penipuan (misalnya, dalam jumlah besar, ke akun yang tidak dikenal, dari geolokasi baru, dll.).

Airome Technologies bersedia berbagi kisah suksesnya, dan berkonsultasi dengan bank tentang aspek teknis dan bisnis.