Sécurité biométrique

Par Patrick Sentinel – 29a.ca

🔐 "Sécurité biométrique : ton doigt, ton visage… et ta naïveté"

Ah, la biométrie c'est futuriste, c'est cool, c'est rapide! Plus besoin de se souvenir de ton mot de passe « T0rtueNinja#1987 ». Tu poses ton doigt, tu montres ton visage… et *hop*, accès total. Comme on dit : « C'est *chill* » mais si tu penses que la biométrie, c'est la fin des piratages... C'est plutôt le début d'un nouvel épisode de *Black Mirror*.

🧠 Ce que tu offres à ton téléphone

- Ton **empreinte digitale** (comme si on n'avait pas assez laissé de traces dans nos textos douteux);
- Ton **visage** (même à 7 h du matin, les yeux collés);
- Ta **voix** (quand tu dis « Ok téléphone, trouve-moi un resto qui ne juge pas mes choix de vie »);
- Et parfois même… ton **iris**, ton **rythme cardiaque**, ou ta **démarche** (oui oui, ton style de marche peut t'identifier, et on ne juge pas… promis 😉).

C'est pratique. C'est magique. Mais le hic?

Contrairement à ton mot de passe… tu ne peux pas *changer de visage* quand il est volé. 😬

🔓 Les vulnérabilités les plus absurdes… et réelles

1. Le doigt imprimé en 3D

Des chercheurs ont déjà réussi à tromper des capteurs d'empreinte avec une fausse empreinte imprimée à partir… d'une photo haute résolution. Donc si tu mets souvent des selfies de ton doigt levé en ligne… pense-y.

2. Le visage en photo

Oui, certains vieux systèmes de reconnaissance faciale se font berner par une **photo imprimée**. Même ton oncle peut t'usurper avec une vieille photo de Noël 1970.

3. La voix clonée

Avec l'IA, il est possible d'imiter ta voix pour tromper des systèmes d'authentification vocale. Ton téléphone pourrait se faire ouvrir par une voix synthétique qui dit juste : *"C'est moi, ouvre-toi banane."*

4. Le hacker bricoleur

Certains ont déjà utilisé **de la colle, du silicone, et un peu de patience** pour créer un faux doigt. À ce niveau-là, ce n'est plus un piratage, c'est de l'artisanat.

🛡️ Alors, on fait quoi ? On retourne au mot de passe "123456" ?

Non. Voici des conseils (semi-sérieux) pour sécuriser ta biométrie :

✅ Active l'authentification multifactorielle (MFA) -> Je le rappelle souvent et ce n'est pas pour rien (*trust me*)

Une empreinte seule, c'est bien. Une empreinte + un code PIN, c'est mieux. Une empreinte + ton chat qui te regarde dans les yeux… bon, on s'égare juste un peu 😉.

✅ Évite les systèmes biométriques non chiffrés

Si ton appareil stocke ton empreinte **en clair**, c'est comme coller une photocopie de ton doigt sur la porte d'entrée. Pas très sécuritaire!

✅ Gère la reconnaissance faciale comme un filtre Instagram

Assure-toi que ton système utilise de la **profondeur**, des points de reconnaissance, et pas juste un selfie flou à 2$.

✅ Évite de partager tes données biométriques inutilement

Non, ton application de karaoké n'a pas besoin de ton empreinte ni de ta fréquence cardiaque.

🧘 Conclusion :

La biométrie, c'est comme confier les clés de ta maison à ton propre corps. C'est pratique. Mais quand ce corps est cloné, photographié ou imprimé en 3D, ça devient un peu… inquiétant.

Alors continue d'utiliser ton doigt ou ton visage, mais fais-le avec prudence. Et rappelle-toi : Ton empreinte est unique. Ta naïveté… malheureusement, non.

Tous droits réservés – https://29a.ca – Patrick Sentinel @ 2025
