FINGERPRINTS

# DISSIPER LES MYTHES ET LÉGENDES DE LA BIOMÉTRIE

Exposer le talon d'Achille des idées reçues sur la biométrie moderne

*La biométrie par empreinte digitale a connu un énorme succès dans les applications grand public telles que les smartphones, les cartes de paiement et les serrures de porte... Cependant, plusieurs mythes et fausses idées entourant la biométrie subsistent aujourd'hui, ce qui peut en limiter l'adoption.*

*Il est temps de remettre les pendules à l'heure et de montrer la qualité, la sécurité et la fonctionnalité réelles des solutions modernes*

# TABLE DES MATIÈRES

# BRISER LE MYTHE

## UN PROJET HERCULÉEN

**DES TRADITIONS ORALES** aux poèmes épiques, en passant par les franchises cinématographiques d'aujourd'hui, l'humanité est captivée par les mythes depuis des siècles. Cependant, la technologie ayant fusionné avec les mythes, il peut devenir difficile de distinguer la réalité de la fiction.

Les industries de la télévision, du cinéma et de la littérature ont créé nos propres mythes du 21e siècle, en cherchant à exciter les téléspectateurs et à intriguer le public, dont beaucoup sont liés au sujet de cet article : la biométrie. Pensez aux espions qui prélèvent des empreintes digitales sur des verres de martini pour usurper l'identité de leurs clients.

Parallèlement, les limites des premières solutions biométriques restent dans l'esprit des consommateurs. Désormais dépassées, ces idées reçues ne reflètent pas la qualité et la valeur des solutions modernes.

Bien qu'il s'agisse souvent d'une simple technique narrative, ces mythes et idées reçues peuvent limiter la foi (et l'adoption !) de technologies qui apportent sécurité et confort à des millions de personnes dans le monde.

L'évolution de la biométrie grand public au cours des deux dernières décennies a été phénoménale - il suffit de voir l'adoption rapide des capteurs d'empreintes digitales sur les smartphones. Il est temps de dissiper certains des mythes courants en matière de biométrie et de montrer à quel point les solutions actuelles sont intelligentes.

# LA BIOMÉTRIE : LA RÉALITÉ

Avant d'aborder les préjugés qui entourent la biométrie, récapitulons rapidement quelques faits marquants sur son utilisation actuelle.

1 | L'empreinte digitale a remplacé les codes PIN et les mots de passe comme moyen d'authentification le plus populaire sur les téléphones portables.

2 | 70 % des smartphones livrés sont équipés de la biométrie, et 82 % des consommateurs qui ont accès à la biométrie sur leur mobile l'utilisent

3 | La biométrie gagne du terrain dans de nouvelles applications et de nouveaux facteurs de forme pour les consommateurs, en tant que moyen d'authentification sûr et pratique.

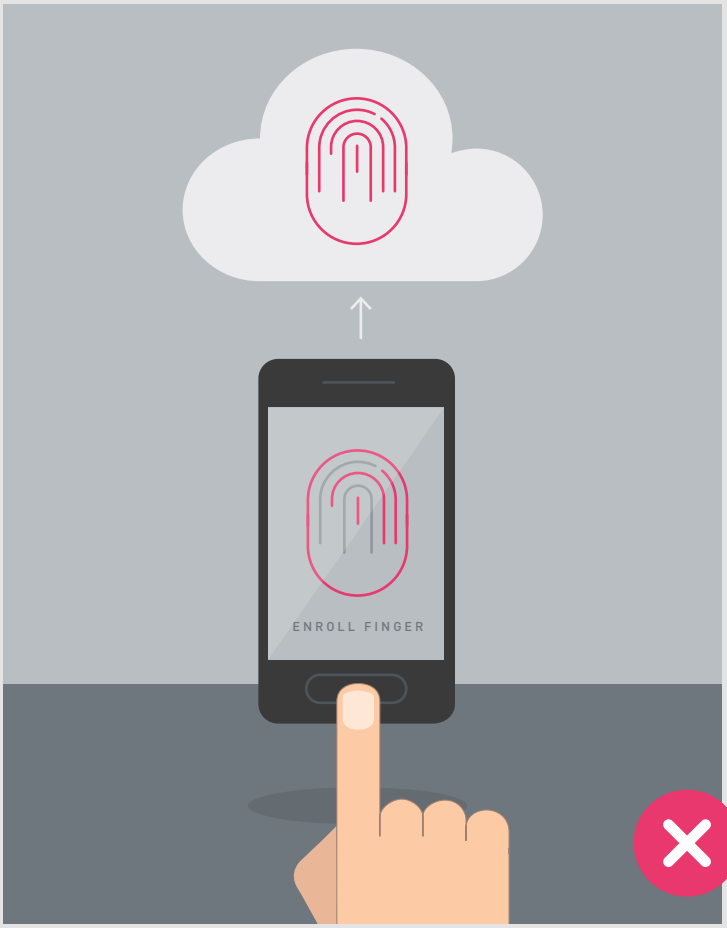
"L'utilisation de **la biométrie** continue de s'étendre au-delà des cas d'usage établis pour atteindre de nouveaux domaines de la vie quotidienne, **transformant la façon dont nous payons, déverrouillons et accédons à notre monde.** Mais avant que la technologie ne puisse atteindre son plein potentiel, nous devons **nous attaquer à certains des principaux mythes et préjugés** et décortiquer la véritable valeur de l'utilisation de nous-mêmes comme clés de nos vies."

**Christian Fredrikson**, CEO de Fingerprints

# MYTHE 01

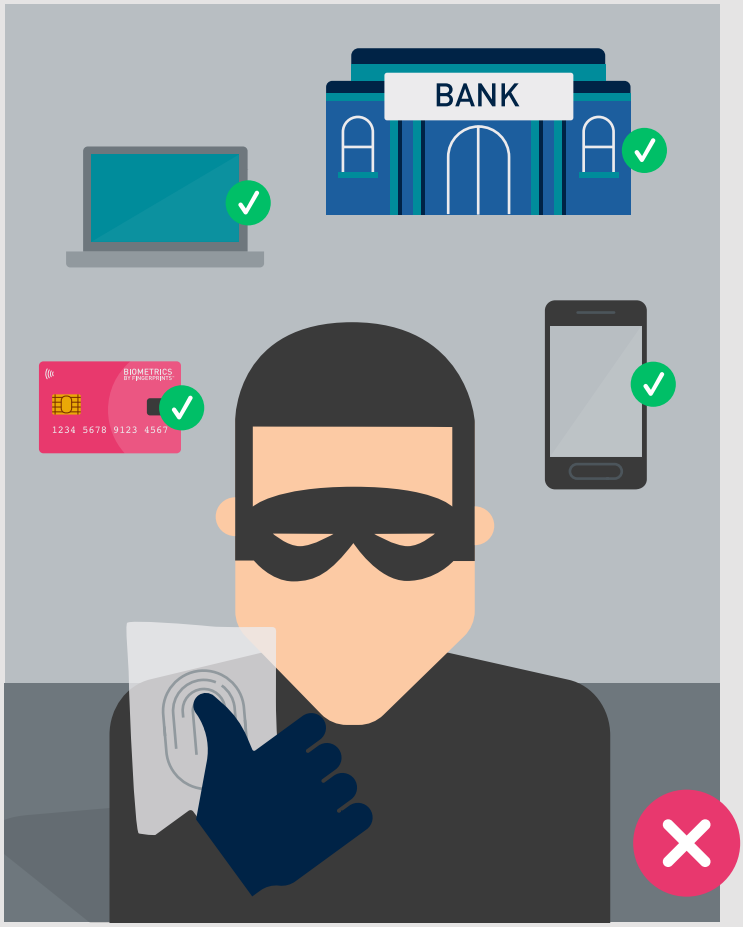
## Les données biométriques sont stockées sous forme d'images dans des bases de données faciles à pirater.

Si l'on y accède, il est définitivement compromis et ne peut être restauré.



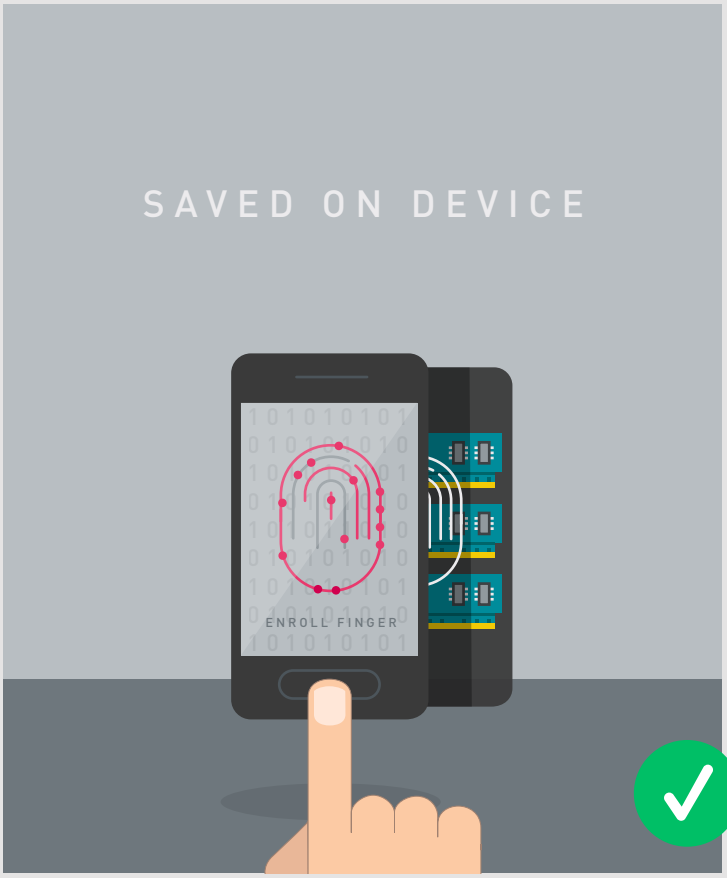

***MYTHE***

Lorsqu'un identifiant biométrique est enregistré sur un appareil, il est stocké sous forme d'image dans une base de données ou un nuage.




***MYTHE***

Si cette image ou ce dispositif est volé, les données biométriques de l'utilisateur sont alors compromises de manière irréversible dans toutes les applications.




***RÉALITÉ***

Les données capturées par un capteur biométrique sont stockées sous la forme d'un modèle en code binaire - en d'autres termes, des 0 et des 1 cryptés. Elles sont stockées sur le dispositif, et nulle part ailleurs.


***RÉALITÉ***

Stockage d'une représentation mathématique, un modèle crypté, plutôt qu'une image, qui ne peut être utilisé ou interprété sur aucun autre appareil.

# LA BOITE DE PANDORE

Pour beaucoup, un des principaux mythes concernant la biométrie est que lorsqu'un identifiant biométrique est enregistré sur un appareil, il est ensuite stocké sous forme d'image. Si cette image est volée, les données biométriques de l'utilisateur sont alors irréversiblement compromises dans toutes les applications. Ce n'est pas vrai.

En réalité, les données capturées par un capteur biométrique sont stockées sous forme de modèle en code binaire - en d'autres termes, des 0 et des 1 chiffrés. Le stockage d'une représentation mathématique plutôt que d'une image rend le piratage considérablement plus difficile.

Les modèles sont irréversibles, de sorte que l'image d'empreinte digitale ne peut pas faire l'objet d'une ingénierie inverse pour recréer l'image d'empreinte digitale originale, même si des pirates s'emparent des données. Le cryptage des données rend impossible la réutilisation d'un modèle d'un dispositif dans un autre. Dans la plupart des applications grand public, le modèle biométrique n'est pas stocké dans un endroit vulnérable situé dans le cloud, il est hébergé en toute sécurité dans le matériel et le logiciel de l'appareil lui-même.

Dans les smartphones, le modèle est stocké, et les algorithmes impliqués dans le processus d'authentification sont exécutés, dans l'environnement d'exécution de confiance (EEC) hautement sécurisé de l'appareil. Toutes les données sont cryptées de manière à ce qu'elles ne puissent être utilisées que sur cet appareil.

La technologie de la puce qui sécurise les données financières de votre carte bancaire, le Secure Element (SE), offre un environnement dynamique pour stocker, traiter et faire correspondre les informations biométriques en toute sécurité pour les cartes de paiement biométriques.

Dans la plupart des cas d'utilisation actuels du contrôle d'accès, tels que l'accès aux bâtiments et les clés USB, les données biométriques requises pour authentifier un utilisateur sont stockées dans le dispositif lui-même, et non dans un emplacement tiers.

Ces solutions matérielles répondent à l'idéal de la sécurité : rendre la tâche suffisamment difficile et les récompenses suffisamment limitées pour que les pirates considèrent que le défi n'en vaut pas la peine

# MYTHE 02

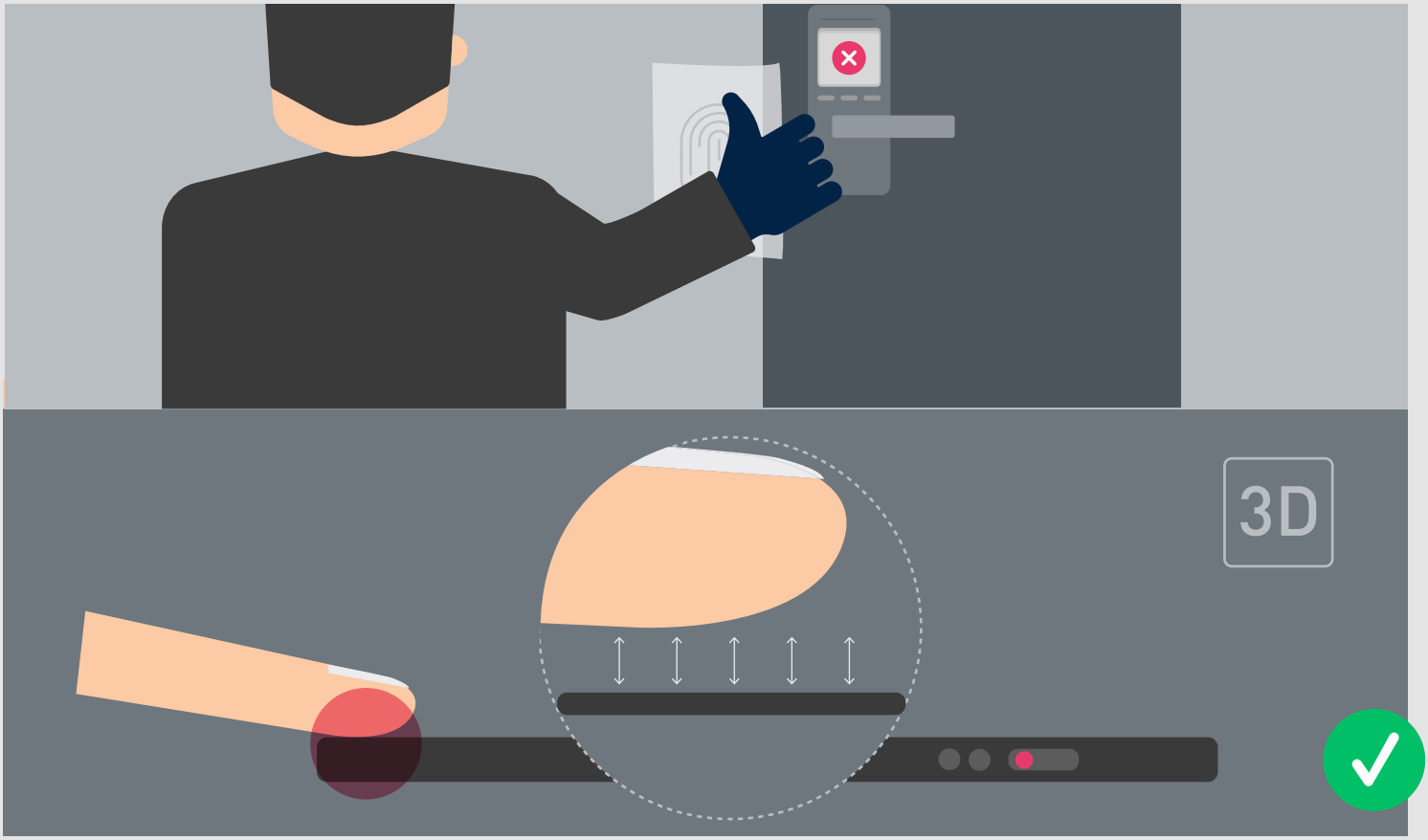
## Les empreintes digitales peuvent être facilement reproduites pour tromper les appareils.

***MYTHE***

Il est facile de créer une contrefaçon 3D à partir de l'empreinte digitale capturée, par exemple, sur un verre que quelqu'un a touché.


***MYTHE***

Il est facile de mettre la main sur les appareils personnels appartenant à la bonne empreinte digitale, sans que le propriétaire s'en aperçoive et le bloque.




***RÉALITÉ***

Des mesures anti-fraude sont désormais incluses en standard, empêchant une empreinte 2D ou une simple usurpation de passer pour un vrai doigt. Vous devez disposer d'informations 3D correctes pour tenter d'obtenir un accès. Non seulement vous avez besoin de la bonne empreinte digitale en 3D, mais vous devez également mettre la main sur le dispositif auquel vous voulez accéder (carte de la personne, smartphone, etc.) avant que la personne ne le remarque et bloque la carte/le téléphone, etc. Ce qui en fait une attaque peu pratique et non évolutive.

## ATTENTION À L'OURS EN GOMME !

Les mythes sont nombreux ici. Qu'il s'agisse de ruban adhésif, d'ours en gélatine ou d'empreintes digitales, beaucoup pensent qu'il est assez simple de simuler un identifiant biométrique pour tromper les dispositifs et obtenir un accès. Ce procédé est connu sous le nom d'usurpation.

Si, par le passé, un ours en gélatine a pu tromper les capteurs, les solutions modernes disposent aujourd'hui de plusieurs défenses sophistiquées qui rendent impossible toute usurpation aussi simple. Les mesures anti-spoofing sont désormais incluses en standard.

Un meilleur logiciel est la clé ici. L'amélioration de la qualité des images capturées et des algorithmes de comparaison permet de défendre les solutions contre des attaques de plus en plus complexes. Le fait est que toutes les certifications des réseaux de paiement et de la FIDO exigent des qualités anti-spoofing testées et prouvées.

Les capteurs les plus récents ne peuvent pas être trompés par une réplique en 2D de l'empreinte digitale capturée à partir d'un objet tel qu'un verre que quelqu'un a touché, car elle a alors perdu toutes ses informations en 3D (par exemple, la profondeur et la hauteur des crêtes et des vallées). Dans la vie réelle, il est extrêmement difficile de créer une copie 3D d'une empreinte digitale qui fonctionnerait efficacement.

De plus, le criminel doit avoir accès à l'appareil de la personne où l'empreinte digitale est enregistrée, par exemple un smartphone ou une carte de paiement, avant de s'en rendre compte et de la bloquer. Ce n'est ni évolutif, ni courant. En comparaison, il est plus facile et plus problématique d'accéder au code PIN d'une personne par-dessus son épaule ou d'utiliser une carte sans contact.

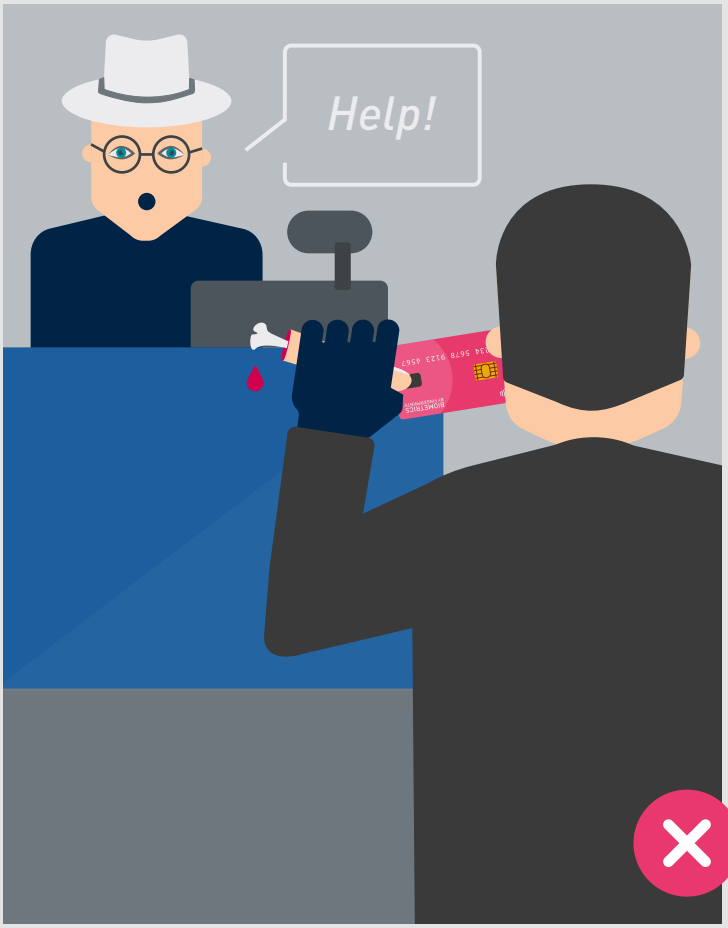
Attention, ce n'est pas pour les âmes sensibles.

# MYTHE 03

## Les doigts détachés sont couramment utilisés pour accéder aux données

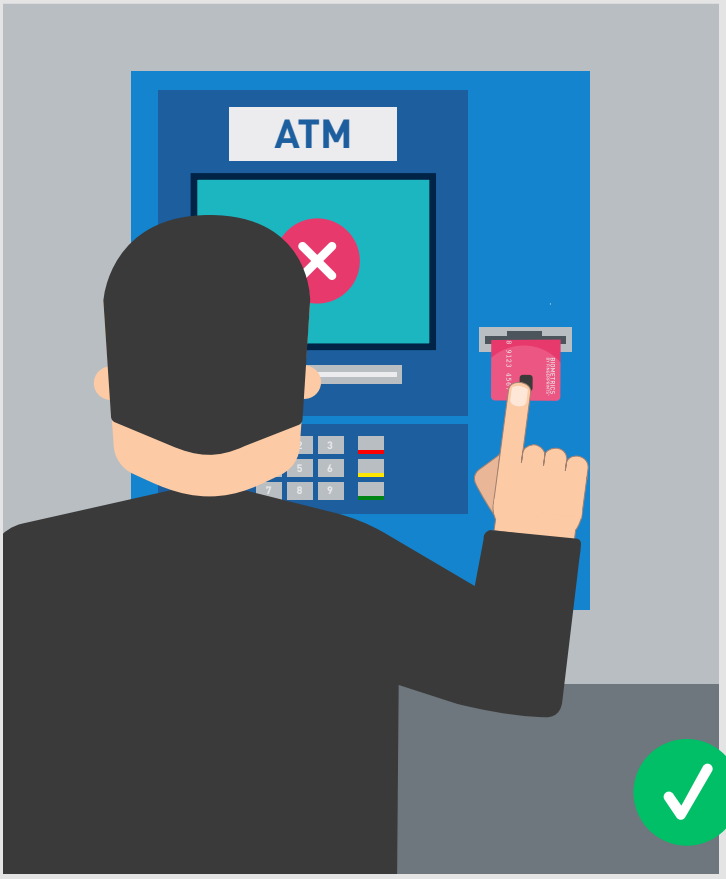
***MYTHE***

Les parties détachées du corps, comme un doigt ou un œil, peuvent facilement être utilisées pour accéder aux données.




***MYTHE***

Comme l'utiliser pour vérifier le paiement avec la bonne carte ou le bon smartphone.


***RÉALITÉ***

Retirer un doigt pour accéder à l'appareil d'une victime (par exemple une carte de paiement) peut être convaincant dans les films mais, en réalité, il s'agit d'un scénario très extrême et peu probable. La fraude emprunte la voie de la moindre résistance et, malheureusement, les criminels disposent de techniques moins complexes, comme la force et la violence, pour accéder aux données.

## UNE REPRESENTATION PEU PROBABLE

Utiliser des doigts sectionnés pour accéder à des pièces verrouillées, un œil arraché pour passer un scanner d'iris ?

La représentation hollywoodienne de la biométrie peut être horrible et convaincante, mais la probabilité qu'elle se produise dans des cas d'utilisation normale de la vie quotidienne des consommateurs est très faible.

Comme indiqué précédemment, les solutions biométriques disposent désormais de moyens sophistiqués pour éviter ce type de risque. En outre, l'attaquant devrait également avoir accès au smartphone de la personne, à sa carte de paiement ou à toute autre application sur laquelle la biométrie est enregistrée. Ce qui en fait un scénario très extrême et peu probable.

Les attaques par ingénierie sociale, qui consistent à inciter la victime à donner son code PIN ou son mot de passe, sont beaucoup plus courantes. La biométrie protège complètement contre ces attaques, car la caractéristique biométrique ne peut être transmise.

# MYTHE 04

## Les nouveaux facteurs de forme biométriques doivent être équipés d'une batterie et doivent être rechargés

tous comme les cartes de paiement et d'accès


***MYTHE***

Les nouveaux facteurs de forme biométriques, tels que les cartes de paiement et d'accès, nécessitent des piles et des recharges.


***RÉALITÉ***

Pour les cartes de paiement, les capteurs à très faible consommation sont capables de fonctionner avec l'énergie captée par le terminal de paiement et le champ NFC, de la même manière que les cartes sans contact sont alimentées aujourd'hui. Cette même technologie à très faible consommation est également utilisée dans d'autres cas d'utilisation sans contact, comme les cartes de contrôle d'accès, les petits badges et les bagues.

## QUI EST RESPONSABLE ICI ?

Cette affirmation semble plausible, voire crédible, mais elle ne l'est pas. Les téléphones portables ont de grosses batteries pour alimenter les capteurs, alors les nouveaux facteurs de forme avec biométrie en ont très certainement besoin aussi ?

Pas vraiment.

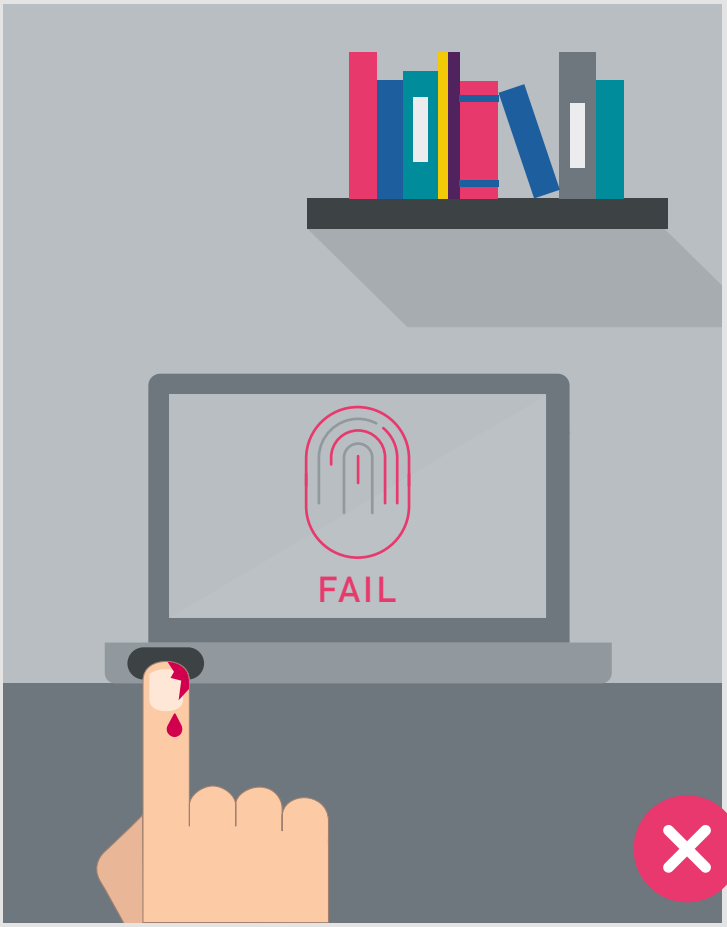
Les experts de l'équipe de R&D ont beaucoup investi pour adapter le capteur mobile éprouvé afin de l'intégrer efficacement dans de nouveaux facteurs de forme plus petits et moins puissants.

La carte de paiement biométrique en est un excellent exemple. Désormais, les capteurs à très faible consommation peuvent fonctionner grâce à l'énergie collectée par le terminal de paiement et le champ NFC, de la même manière que les cartes sans contact sont alimentées. Les cartes de paiement biométriques n'ont donc plus besoin de batterie et peuvent offrir la même expérience utilisateur que les cartes sans contact, mais avec une sécurité accrue!

Cette même technologie à très faible consommation est également utilisée pour d'autres applications sans contact, telles que les cartes de contrôle d'accès, les petits badges et les bagues.

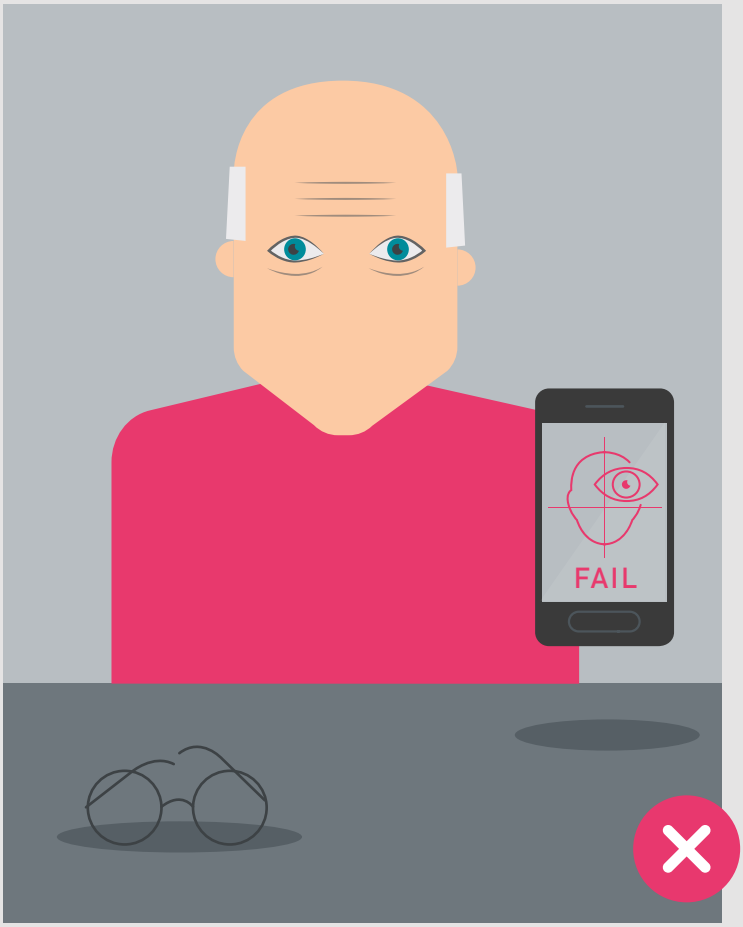
# MYTHE 05

## Si je change avec l'âge, ou si je me fais opérer, je serai bloqué par mes propres biométriques



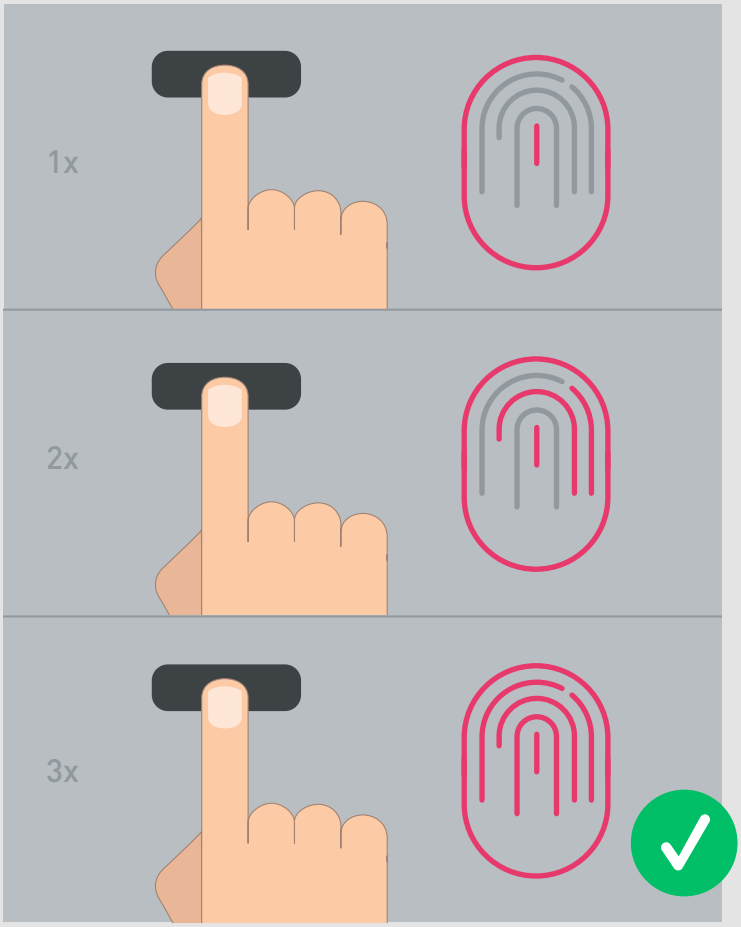

***MYTHE***

Si je me coupe le doigt, je ne pourrai pas accéder à mes appareils.



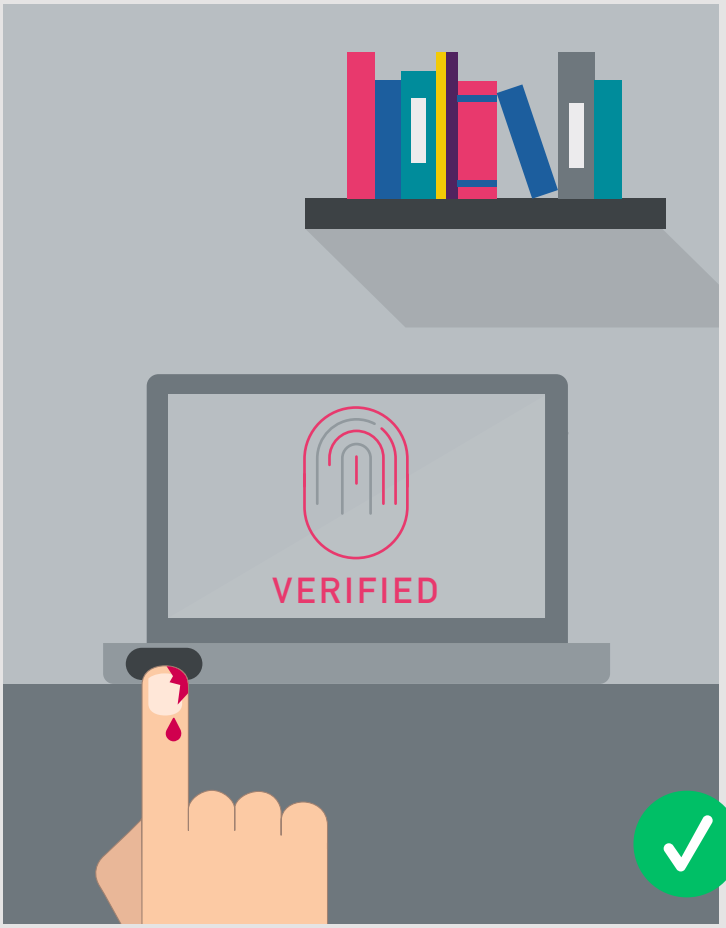

***MYTHE***

Lorsque je changerai avec l'âge, je serai bloqué par mes propres biométriques.




***RÉALITÉ***

La technologie biométrique moderne comporte des algorithmes intelligents d'"auto-apprentissage". Ainsi, lorsque vous touchez le capteur, une nouvelle zone est apprise à chaque fois. Par conséquent, même si vous vous blessez une partie du doigt, l'appareil vous connaît suffisamment bien pour vérifier que c'est bien vous avec la partie restante de votre empreinte digitale.




***RÉALITÉ***

Les changements progressifs qui surviennent au fil des ans - comme le vieillissement des mains ou des yeux - peuvent être pris en compte et sont intégrés dans les modèles dans le cadre des algorithmes d'auto-apprentissage.

## VIEILLISSEMENT

Beaucoup pensent qu'une fois les données biométriques capturées, elles restent statiques. Par conséquent, toute modification de leur situation physiologique les empêchera d'accéder à leurs appareils. Mais ce n'est pas tout à fait vrai.

Comme on peut s'y attendre, de graves changements dans la nature physiologique d'une personne affectent sa capacité à utiliser les données biométriques. En revanche, les changements progressifs qui surviennent au fil des ans, comme le vieillissement des mains ou la débilité des yeux, peuvent être pris en compte.

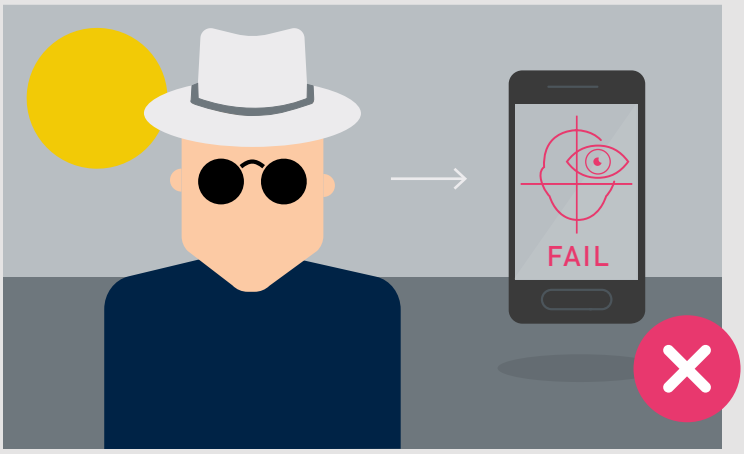
La technologie biométrique moderne est dotée d'algorithmes intelligents "d'auto-apprentissage". Cela signifie qu'ils se mettent à jour et intègrent les évolutions au fur et à mesure qu'elles se produisent. Ils peuvent également prendre en compte les micro-coupures. La plupart des changements cosmétiques n'ont pas d'incidence sur les points de reconnaissance clés utilisés par les systèmes biométriques.

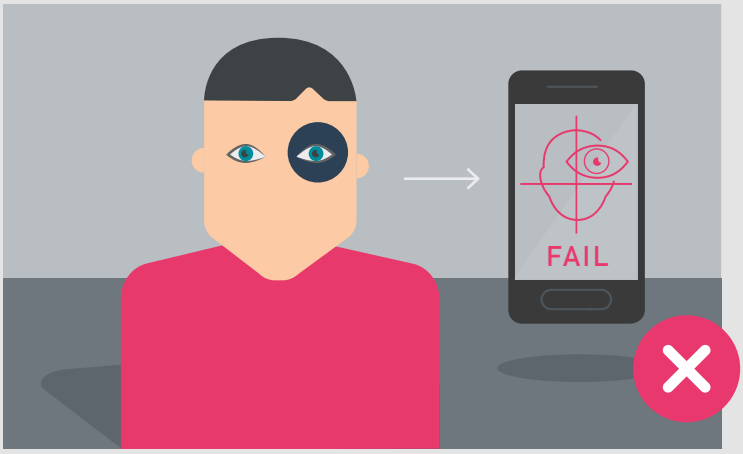
# MYTHE 06

## Les changements environnementaux vont m'empêcher d'accéder à mon appareil

comme des doigts mouillés ou secs, le port de lunettes ou l'exposition au soleil.

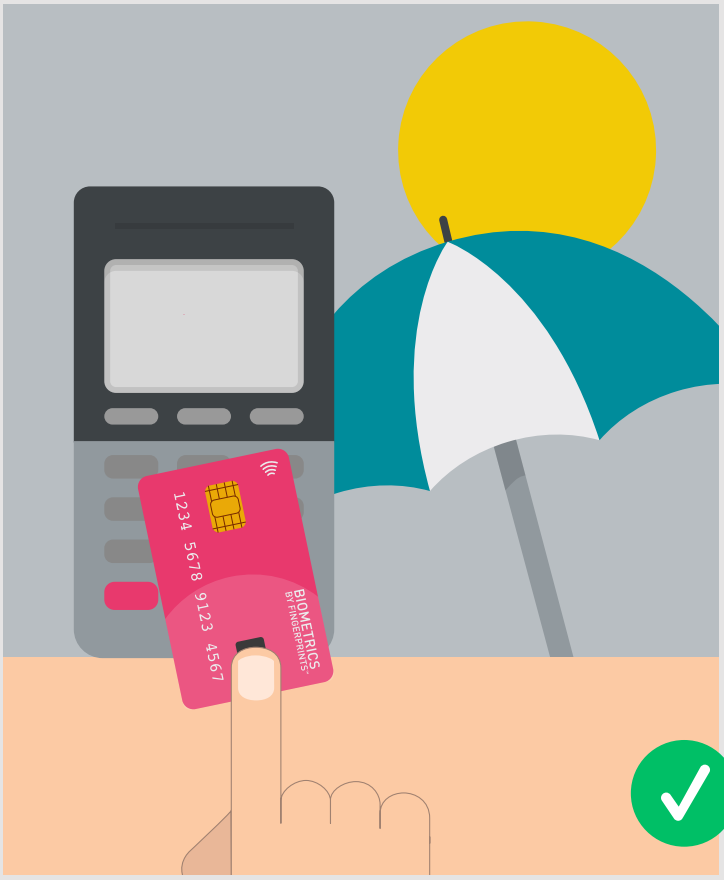


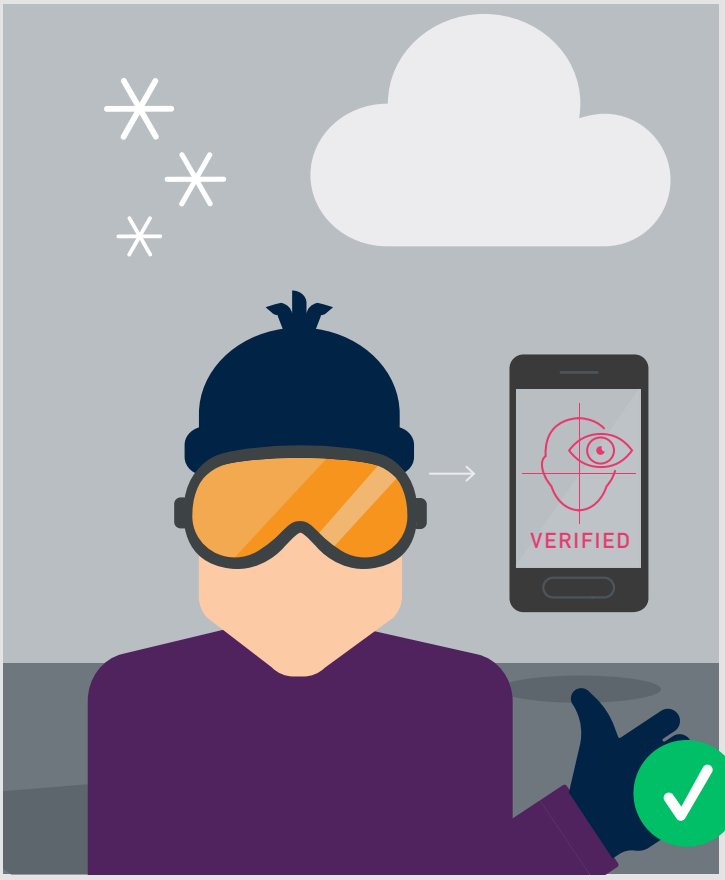



***MYTHE***

Des changements environnementaux et temporaires m'empêcheront d'accéder à mon appareil, comme des doigts secs ou mouillés, le port de lunettes de soleil, une journée froide ou même un œil au beurre noir ou un cache-œil.




***RÉALITÉ***

Ces dernières années, les fournisseurs de solutions biométriques ont investi des millions en R&D pour s'assurer que les utilisateurs puissent toujours être reconnus en cas de changement de climat ou d'environnement. En combinant plusieurs identifiants biométriques, les utilisateurs peuvent surmonter différentes conditions en utilisant une autre forme - par exemple, en utilisant la reconnaissance sans contact du visage ou de l'iris au lieu de l'empreinte digitale.

## LE TEMPS CHANGENT CONTINUELLEMENT

Au cours des dernières années, les fournisseurs de solutions biométriques ont investi des millions dans la R&D afin de garantir que les utilisateurs puissent toujours être reconnus lors de changements de climat ou d'environnement. Qu'il s'agisse de l'adaptation de la reconnaissance du visage et de l'iris à la lumière du soleil ou de la capacité d'un scanner d'empreintes digitales à lire un doigt froid, des améliorations majeures ont été apportées pour minimiser les TFR (taux de faux rejets - le nombre de fois où le bon utilisateur est rejeté à tort).

C'est également là qu'interviennent les algorithmes intelligents, qui apprennent et s'adaptent aux petits changements que peut subir votre empreinte digitale lorsqu'elle est trop chaude ou trop froide, par exemple.

Les solutions biométriques multimodales jouent déjà un rôle dans la lutte contre le verrouillage temporaire. En combinant plusieurs identifiants biométriques, les utilisateurs peuvent surmonter différentes conditions en utilisant une autre forme - par exemple, en utilisant la reconnaissance sans contact du visage ou de l'iris au lieu de l'empreinte digitale.

BIOMETRIE

# L'ACCUEIL D'UN HERO

**A LA DIFFERENCE DES DEMONS ET DES DRAGON**, la croyance dans la valeur de la biométrie ne fait que croître.

Les progrès de la biométrie ont dépassé bon nombre des hypothèses relatives à la limitation des fonctionnalités, de la sécurité ou de la complexité. Si certains mythes subsistent, les consommateurs sont de plus en plus nombreux à s'approprier ces avancées et à comprendre la valeur que la biométrie peut apporter à leur vie quotidienne.

Cela se traduit par l'extension de la biométrie à de nouveaux marchés et cas d'utilisation. Les paiements en sont un bon exemple, les cartes de paiement biométriques étant un facteur de forme en plein essor. Cependant, comme nous l'avons vu, de nouveaux mythes émergent également dans ce domaine...

FingerprintsTM est un leader de l'innovation en biométrie depuis deux décennies. Nous sommes fiers de l'expertise et de la recherche et du développement qui ont permis à notre gamme de solutions biométriques d'offrir une sécurité renforcée et un meilleur confort d'utilisation.

À mesure que les solutions se développent et se diversifient, la lutte contre les mythes va se poursuivre. Mais une chose est sûre : l'avenir de la biométrie est une histoire à ne pas manquer.

# A PROPOS

## ENTREPRISE DE CONFIANCE

- Les capteurs d'empreintes digitales authentifient les appareils des milliards de fois par jour
- Des centaines de millions de capteurs livrés chaque année
- Intégré dans plus de 400 modèles de smartphones

## PERFORMANCE EXCEPTIONNELLE

- Les meilleures mesures de sécurité et de précision de leur catégorie
- Une faible consommation d'énergie inégalée
- Qualité d'image élevée - performances biométriques optimisées pour les petits capteurs

## AMÉLIORER LES POSSIBILITÉS DE CONCEPTION

- Nos petits capteurs, associés à des logiciels, permettent aux marques d'être aussi créatives qu'elles le souhaitent
- Sensors in different sizes, shapes and colors
- Ready for cost-effective, high volume production

L' ETAPE HISTORIQUE

# 1 BILLION SENSORS

1 MILLIARD DE CAPTEURS
EXPÉDIÉS A ÉTÉ ATTEINT EN MAI 2019

4 0 0 +

MO DÈ LE S

D ' AP PA RE IL

M O B I L E

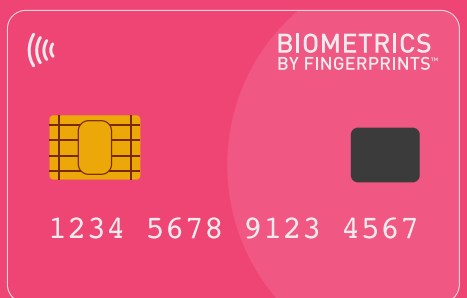
! ! ! ! ! !

## 21 SUR 21

PILOTES DE CARTES DE PAIEMENT
BIOMÉTRIQUES SANS CONTACT

## 1 SUR 1

LANCEMENT COMMERCIAL




NOTRE PRODUIT EXISTE DANS + DE

# + 100

DIFFÉRENTS DISPOSITIFS
D'ACCÈS ET APPLICATIONS

FINGERPRINTS