



CYBERSÉCURITÉ DES JOURNALISTES

@fs0c131y



x

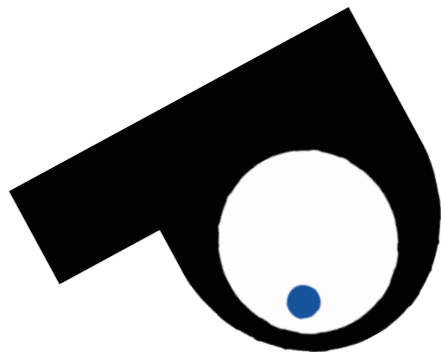
PREDICTA
LAB

QUI SUIS-JE?



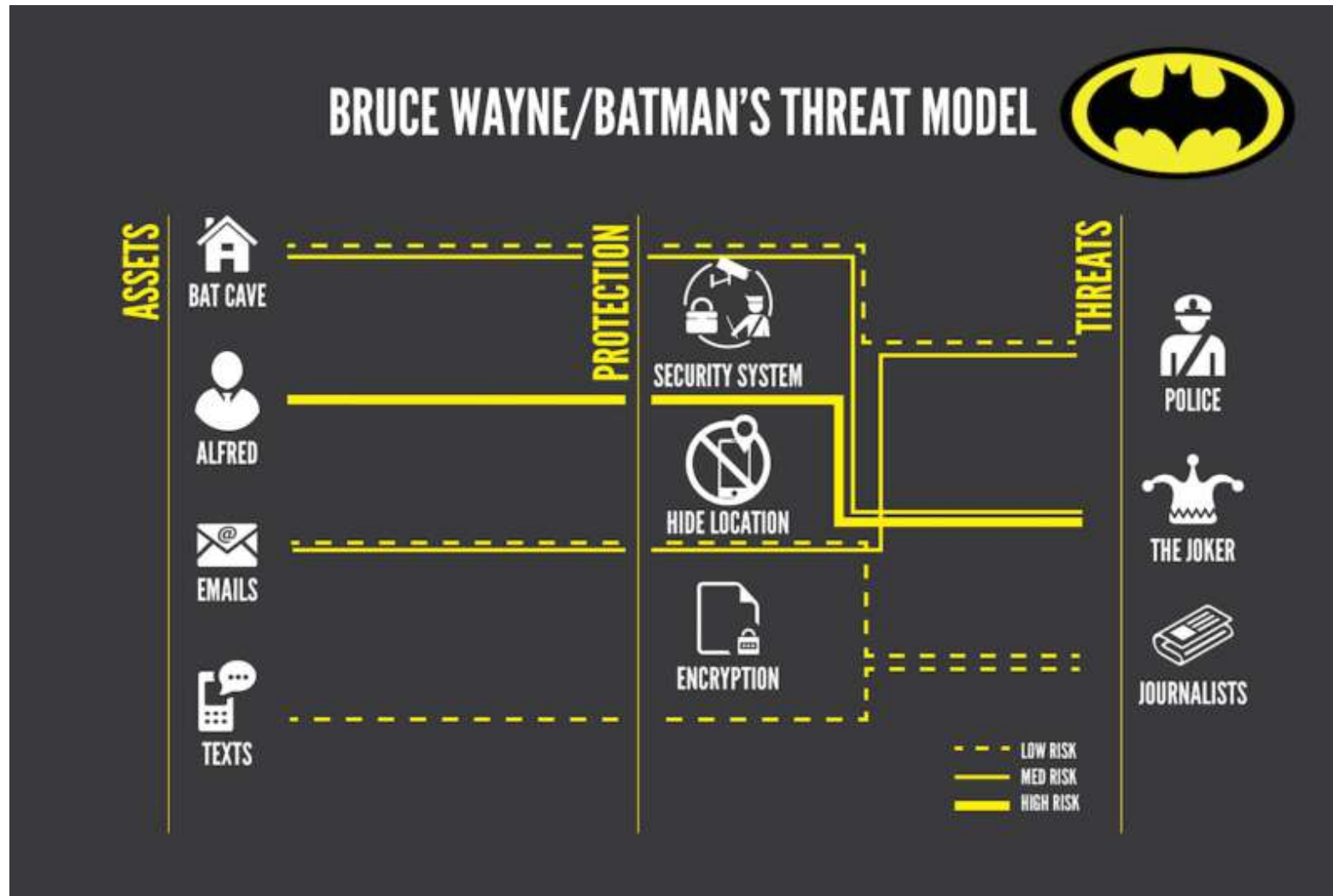
@fs0c131y

-
- **Co-fondateur et président** de Predicta Lab
 - **Hacker éthique français**
 - **Un peu trop de followers** sur Twitter
 - J'aime casser des choses, particulièrement les applications Android



**PRINCIPES
GÉNÉRAUX DE SÉCURITÉ**

MODÈLE DE MENACES

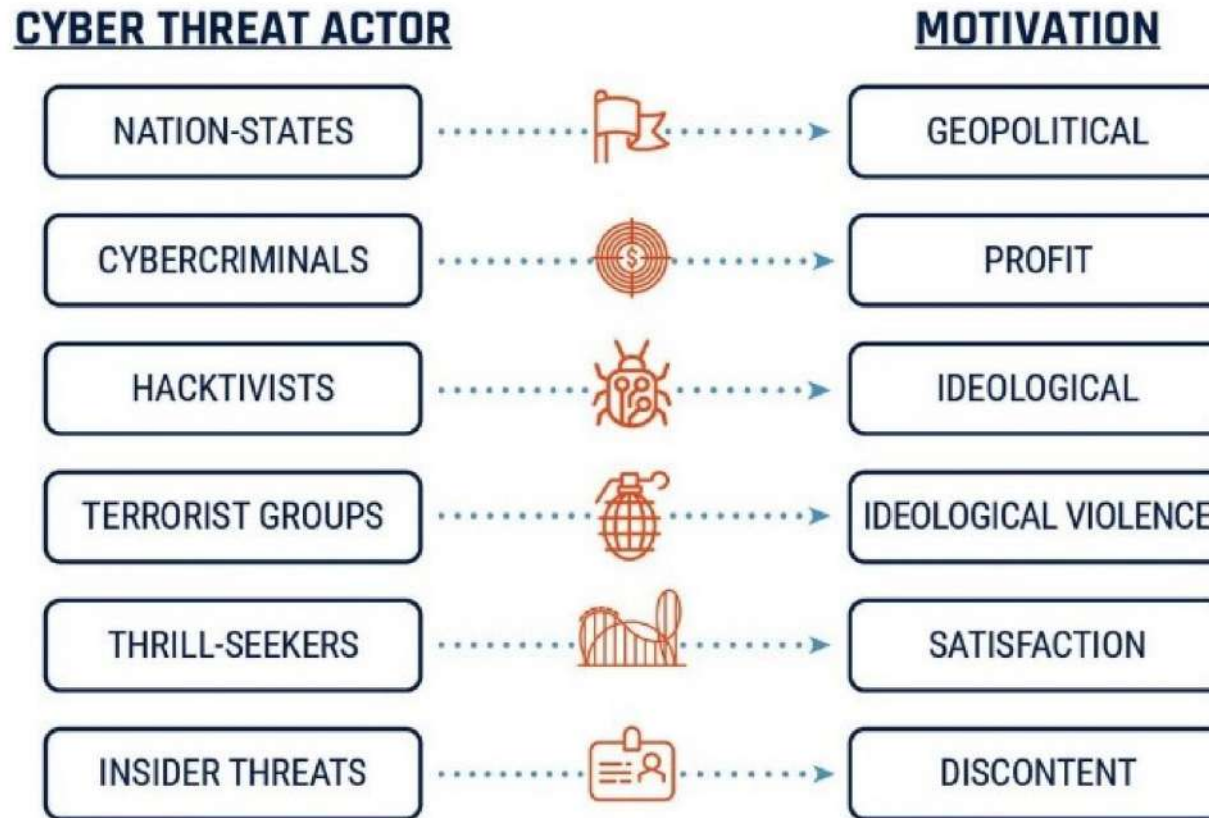


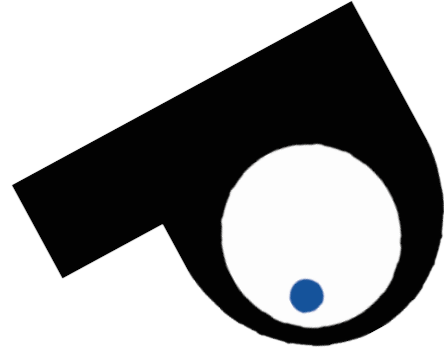
SURFACE D'ATTAQUE



ACTEURS DE LA MENACE

CYBER THREAT ACTORS





MÉTHODES D'INFECTION

INFECTION PAR SMS



Source: [Citizen Lab](#)

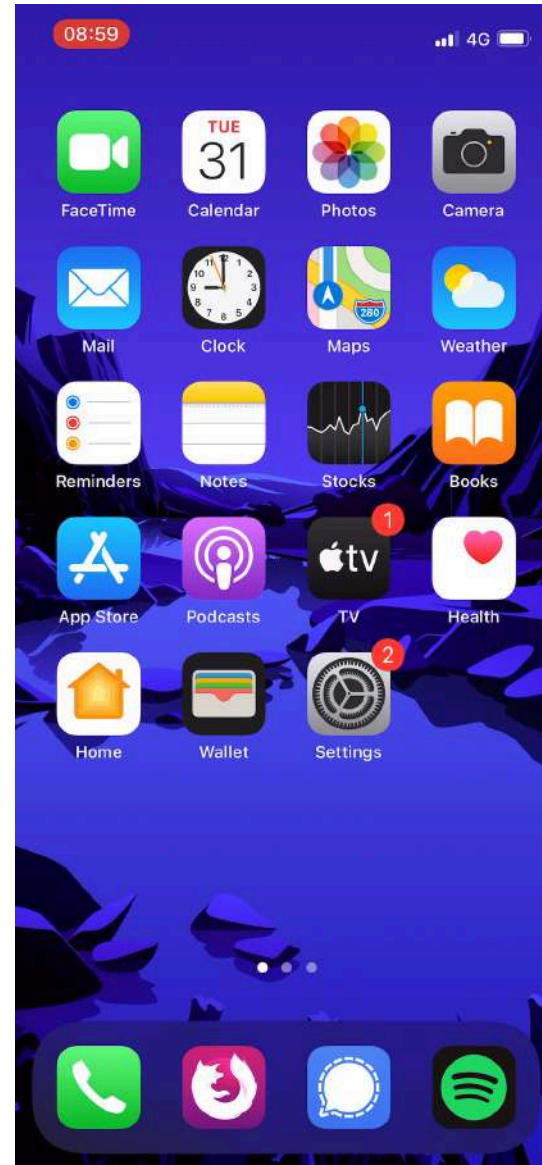


Source: [Bahraini blogger Yusuf Al-Jamri](#)

INFECTION PAR QR CODE



INFECTION PAR QR CODE



INFECTION PAR EMAIL

Your package id43613



DHL Support <harper@polytype-usa.com>

Sun 12/01/2020 06:04

You ▾

[To view this email as a web page, go here](#)



[Help Center](#)

Welcome to MyDHL+ - your one stop for international shipping! You'll be able to create and manage shipments, get quotes, schedule pickups, view reports and more!

Your package id43613

[MyDHL+ id43613](#)

We look forward to supporting your shipping needs!

Regards,

MyDHL+ Team

Please do not reply to this email - inbox is not monitored.



[Terms of Use](#) | [Privacy Notice](#) | [Terms and Conditions of Carriage](#)

2020 © DHL

TYPOSQUATTAGE

amazon.com

VS

amazon.com

ZPHISHER



Sign in
Stay updated on your professional world


Email or Phone


Password [show](#)

[Forgot password?](#)

[Sign in](#)

or

 [Sign in with Google](#)

 [Sign in with Apple](#)

New to LinkedIn? [Join now](#)

CONSEILS GÉNÉRAUX

- Soyez conscients de votre **empreinte numérique**
- **Ne cliquez pas sur les liens suspects** et ne téléchargez pas d'applications inconnues
- Activez les **mise à jour automatiques**
- Utilisez des **mots de passes robustes et différents** pour chaque compte
- Connectez vous à des réseaux **Wi-Fi sécurisés**

SMARTPHONES



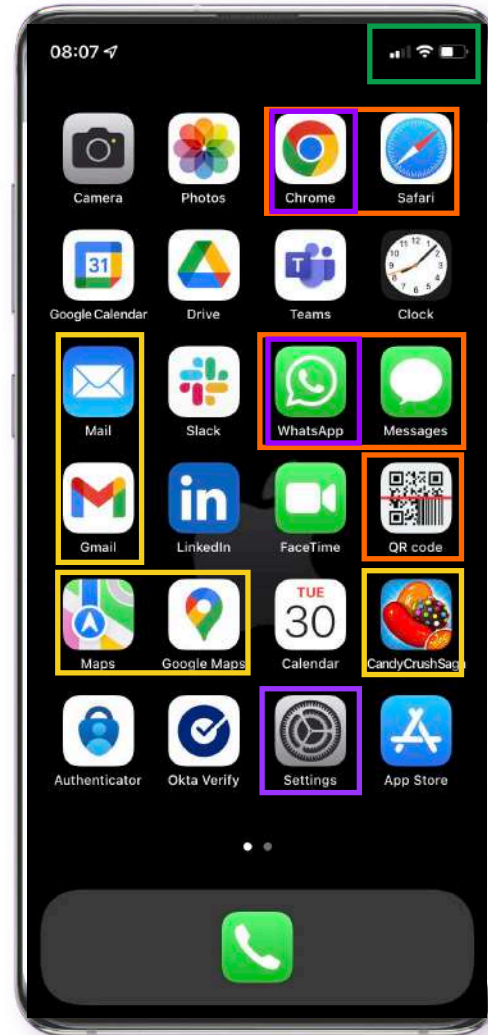
SURFACE D'ATTAQUE SUR SMARTPHONE

Réseaux WiFi non sécurisés

Mélange d'applications professionnelles et personnelles

Applications qui fuient ou transfèrent des données

Applications ou systèmes pas mis à jour



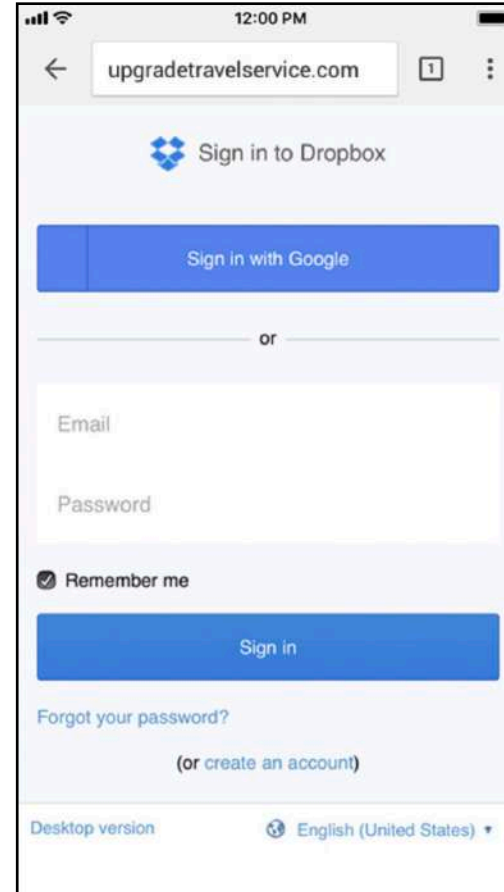
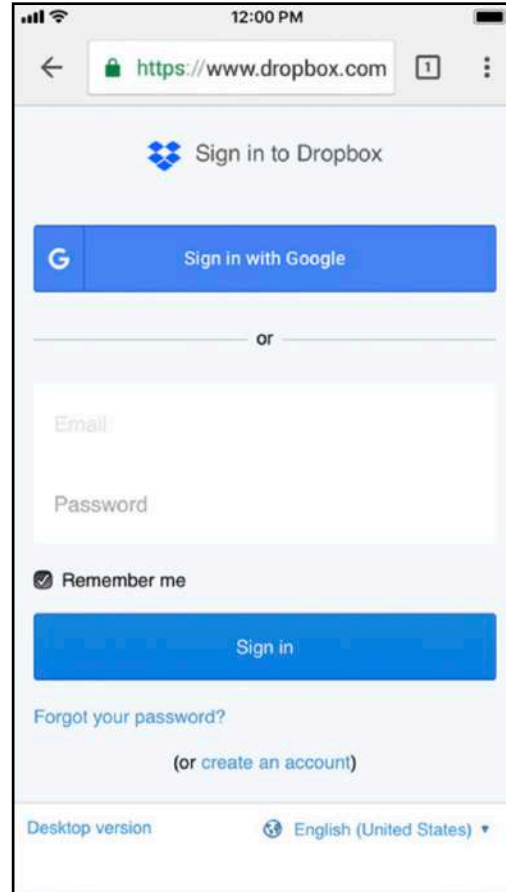
Contenu web malveillant

Attaques de phishing

Scan de QR codes

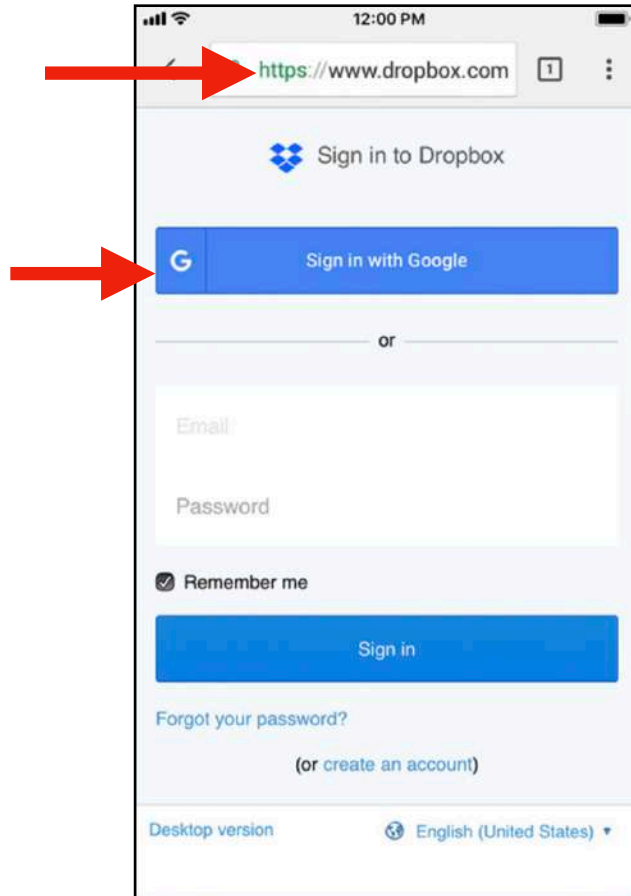
Applications téléchargées en .apk

PHISHING

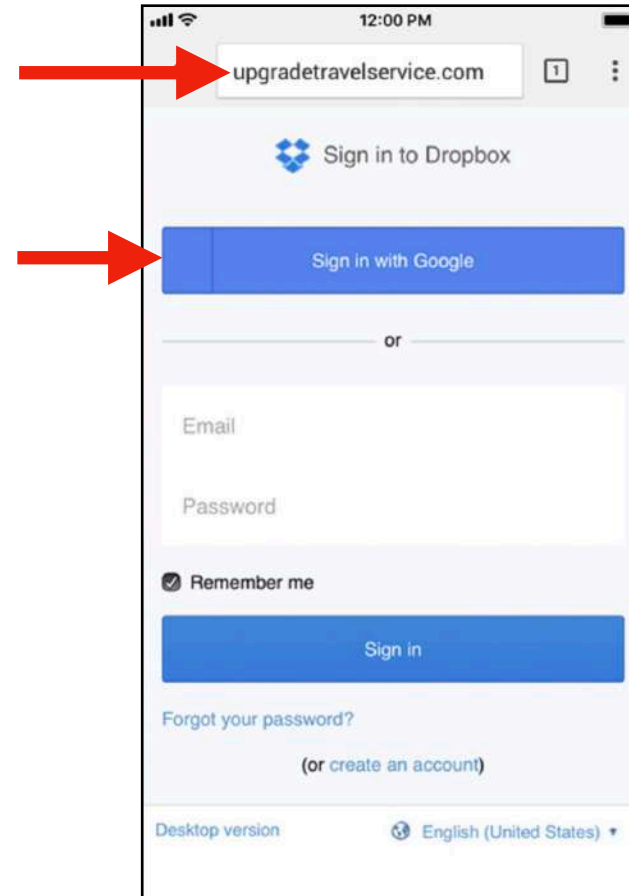


Pouvez-vous trouver les différences entre ces deux sites ?

PHISHING



VRAI



FAUX

TÉLÉCHARGEMENT

D'APK



PLAYSTORE

The screenshot shows the Google Play Store interface. At the top, there are navigation tabs for 'Jeux', 'Applications', 'Films et TV', 'Livres', and 'Enfants'. Below these are device filters: 'Mobile', 'Tablette', 'Séries', 'Chromebook', 'Montre', and 'Voiture'. The main section is titled 'Meilleurs classements' and has three sub-sections: 'Top des applications gratuites', 'Les plus rentables', and 'Top des applications payantes'. The 'Top des applications gratuites' section lists the following apps:

Rang	App	Catégorie	Note
1	TEMU: Shop Like a Billionaire	Shopping	4,7 ★
2	SHEIN-Achats de mode en ligne	Shopping	4,7 ★
3	TikTok	Réseaux sociaux	4,4 ★

The 'Top des applications payantes' section lists the following apps:

Rang	App	Catégorie	Note
4	WhatsApp Messenger	Communication	4,3 ★
5	Instagram	Réseaux sociaux	4,0 ★
6	Cash App	Finance	4,6 ★
7	Snapchat	Communication	4,2 ★
8	AliExpress	Shopping	4,5 ★
9	Messenger	Communication	4,1 ★

The 'Applications populaires' section shows a row of app icons with their names and ratings:

App	Note
WhatsApp Messenger	4,3 ★
Instagram	4,0 ★
Facebook	3,3 ★
TikTok	4,4 ★
Messenger	4,1 ★
Netflix	4,4 ★
Twitter	4,0 ★
Snapchat	4,2 ★

<https://play.google.com/store/apps>

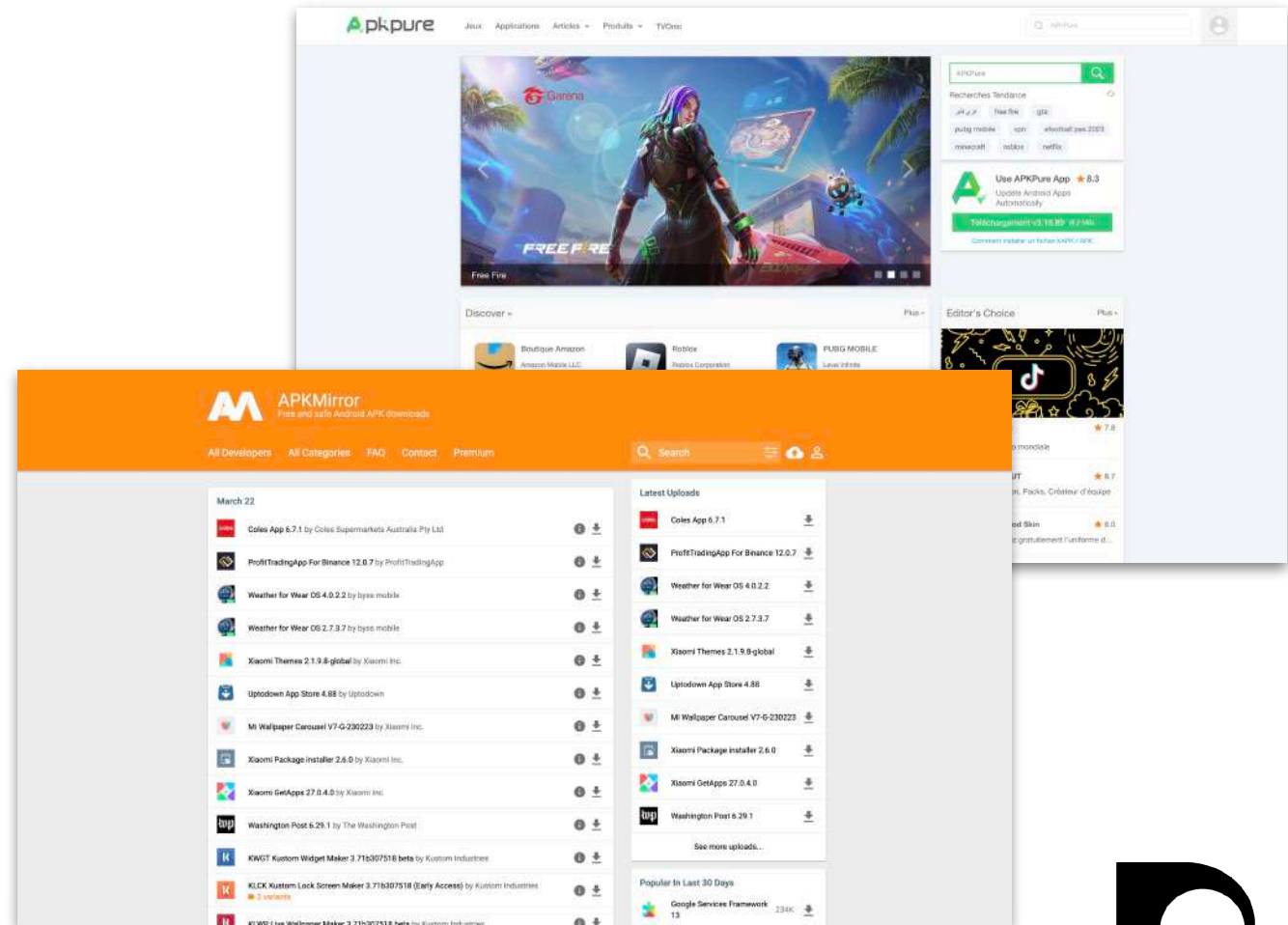
TÉLÉCHARGEMENT D'APK

APKMirror: apkmirror.com

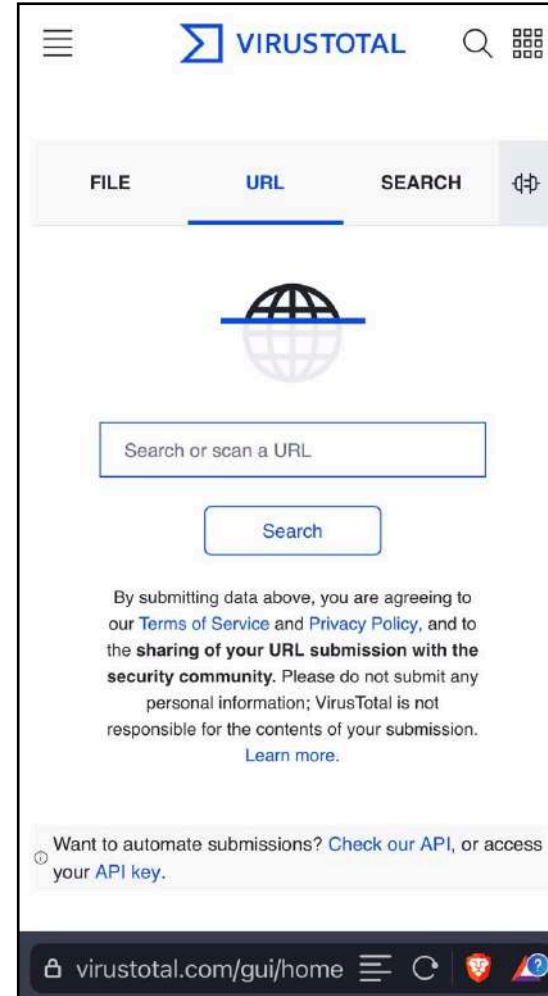
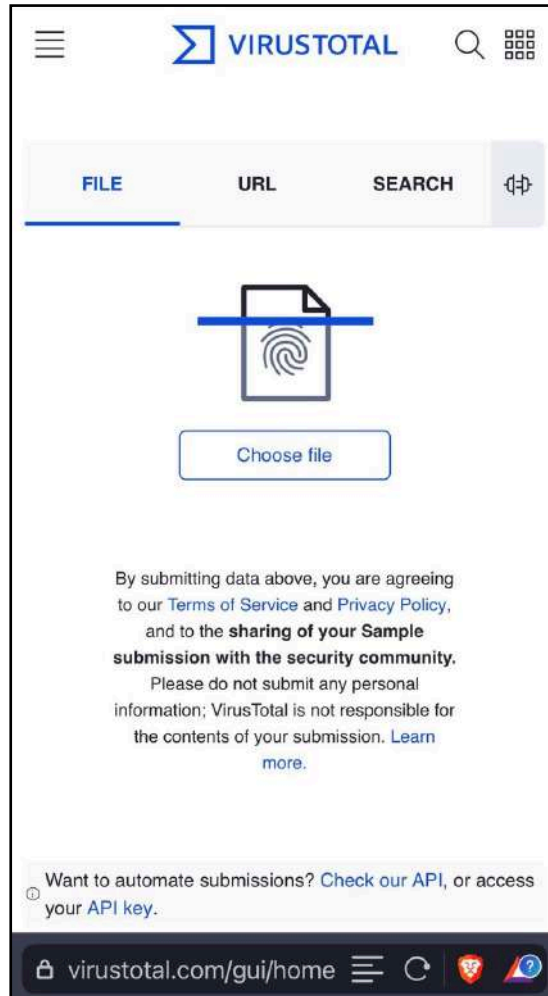
- Les fichiers sont vérifiés avant publication
- Les apps téléchargées sur APKMirror sont mises à jour automatiquement quand le site récupère une nouvelle version

APKPure: apkpure.com

- Les fichiers sont vérifiés avant publication
- Les anciennes versions sont disponibles



VIRUSTOTAL



<https://www.virustotal.com>

VIRUSTOTAL

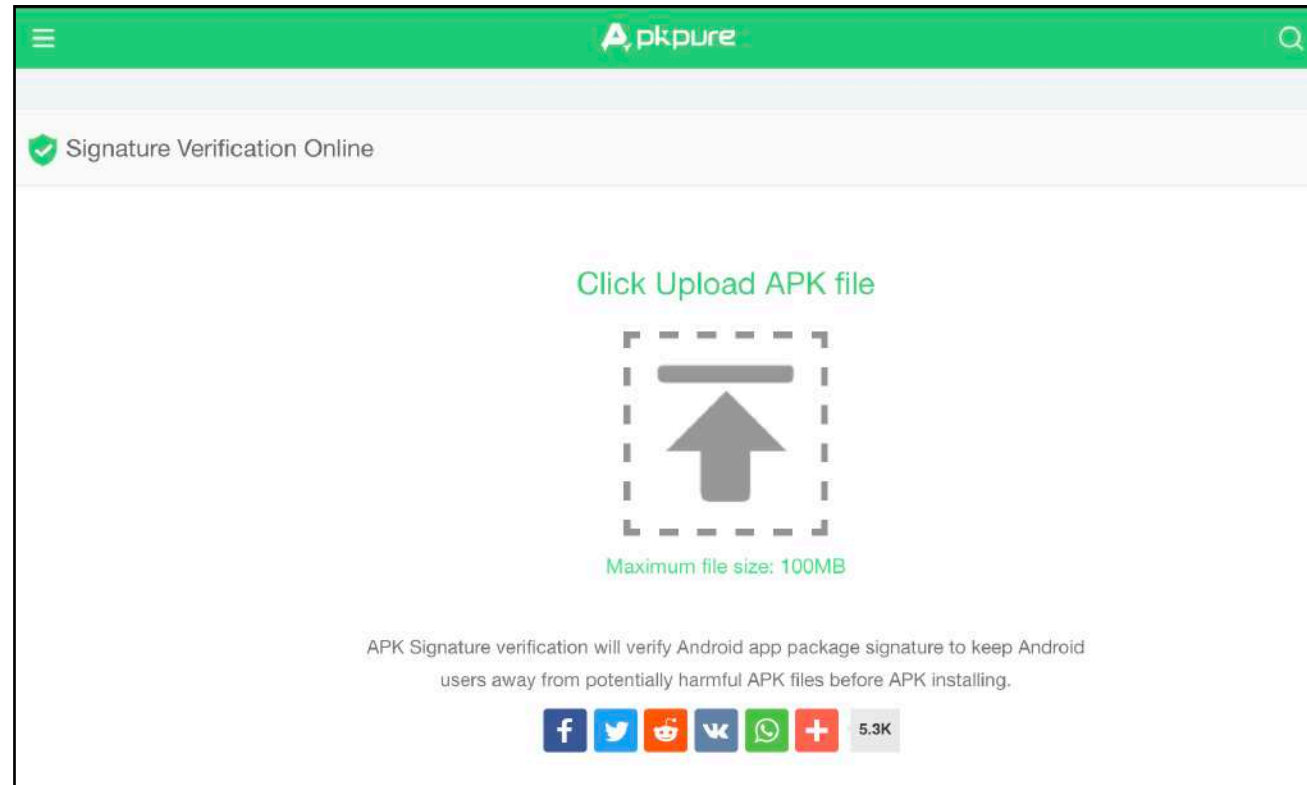
The screenshot shows the VirusTotal website interface. At the top, there is a navigation bar with the VirusTotal logo, a search icon, and a menu icon. Below the navigation bar, there are three tabs: 'DETECTION', 'DETAILS', and 'COMMUNITY'. A blue banner promotes joining the VT Community. Below the banner, there is a section titled 'Security vendors' analysis' with a sub-header 'Do you want to automate checks?'. A table lists various security vendors and their analysis results. A red arrow points from the 'Do you want to automate checks?' question to the text 'NOT OK Je ne clique pas'.

Vendor	Analysis Result
Avira	Phishing
Emsisoft	Phishing
Kaspersky	Phishing
Lionic	Phishing
Netcraft	Malicious
Sophos	Malware
Trustwave	Phishing
Fortinet	Spam
Abusix	Clean
Acronis	Clean
ADMINUSLabs	Clean
AICC (MONITORAPP)	Clean

NOT OK
Je ne clique pas

VÉRIFICATION DE SIGNATURE

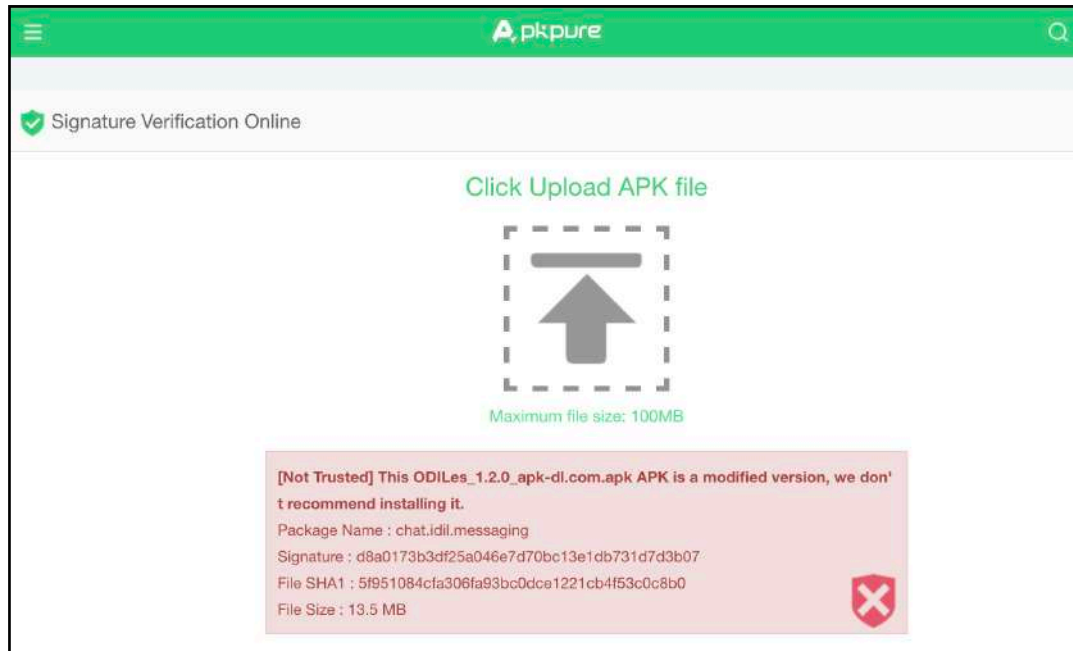
APKPURE



<https://apkpure.com/apk-signature-verification>

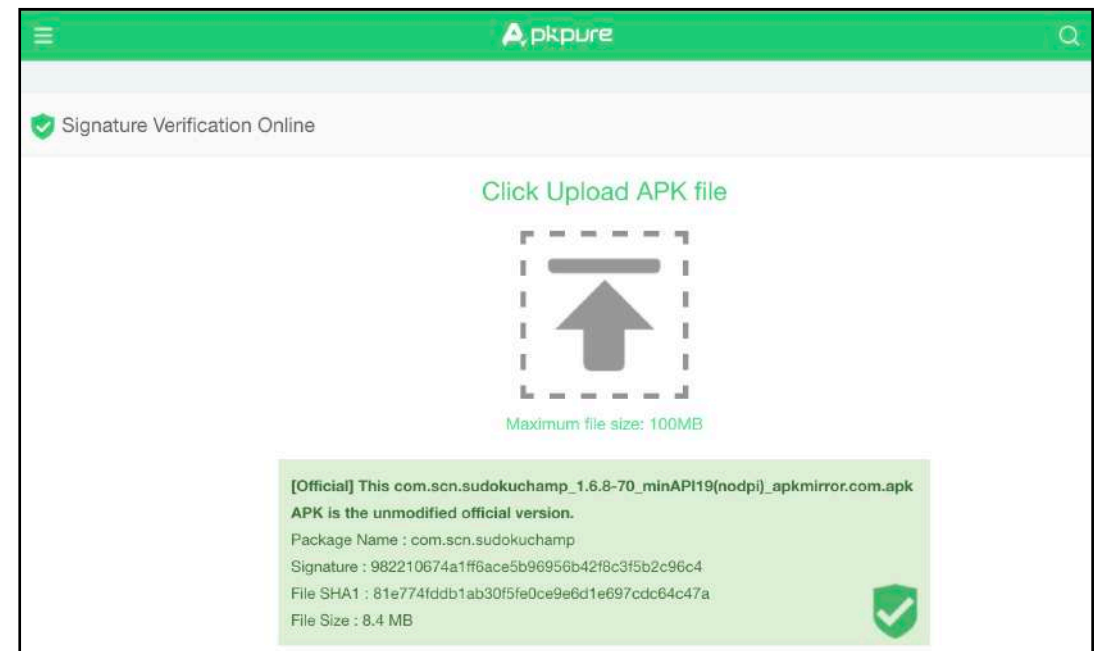
VÉRIFICATION DE SIGNATURE

APKPURE



NOT OK

Je ne dois pas installer l'app



OK

Je peux installer l'app

APPLICATIONS

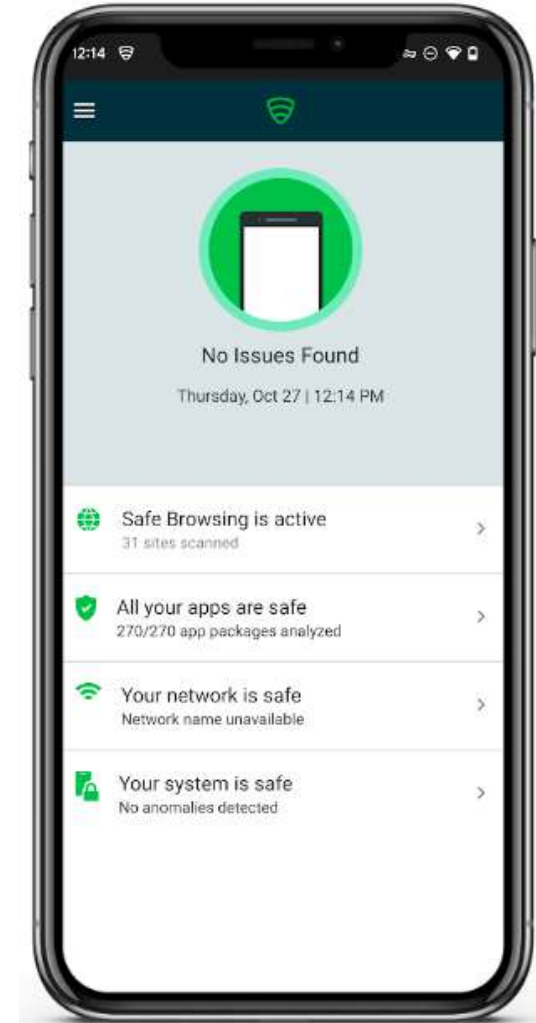


LOOKOUT FOR WORK



Lookout est une application mobile tout-en-un pour la protection contre le contenu malveillant en ligne.

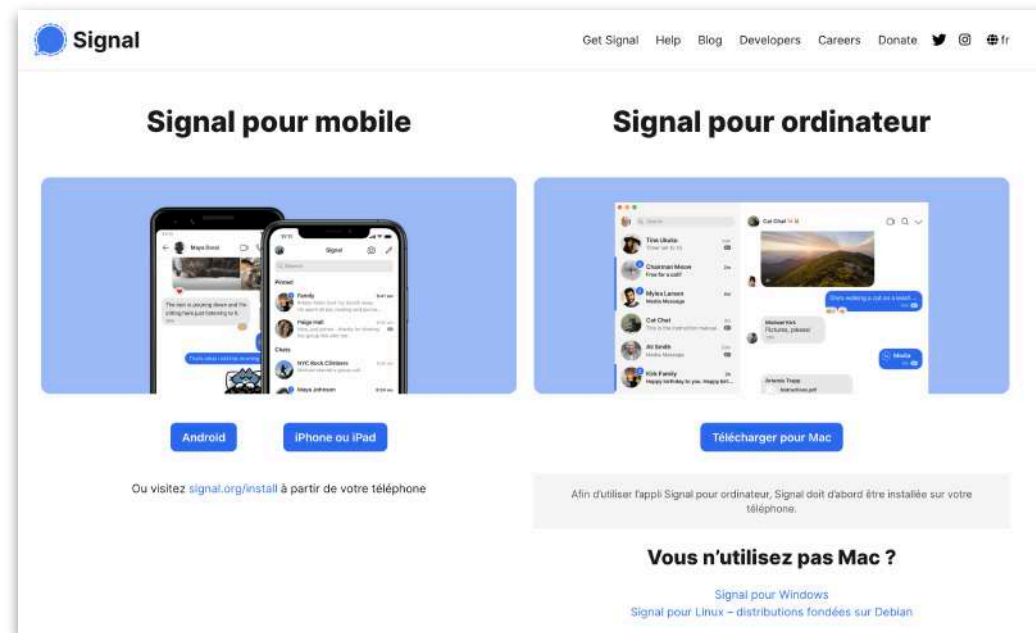
- Navigation sûre
- Wi-Fi sûre
- Alerte piratage
- Analyseur de système



APPLICATIONS DE MESSAGERIE



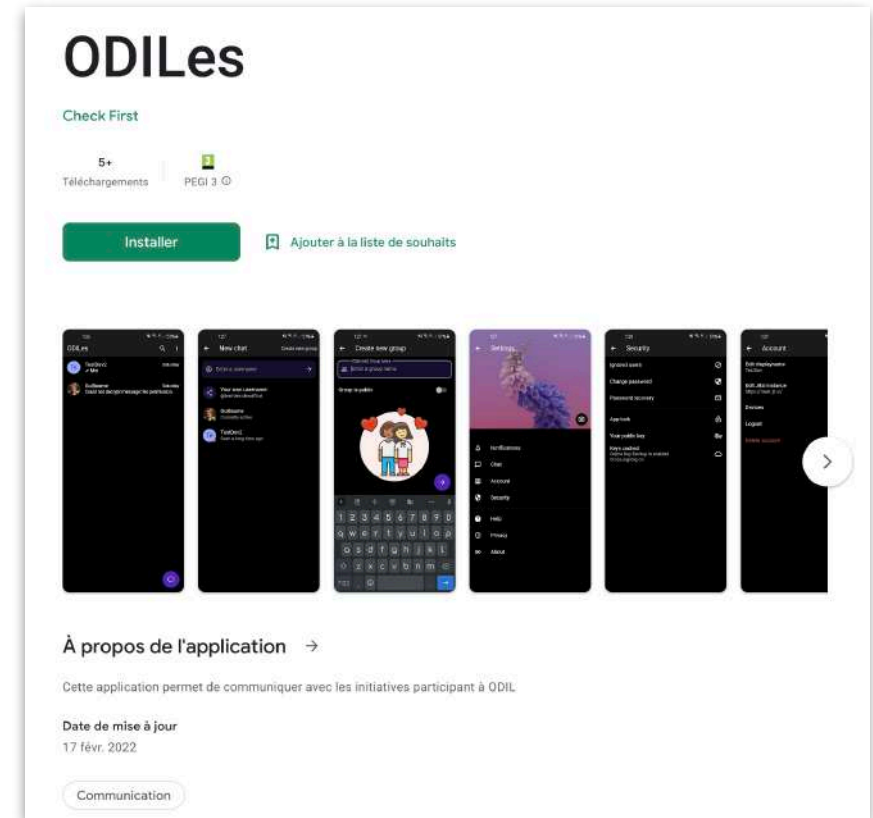
- **Un chiffrement de bout en bout** (propulsé par le protocole Signal à code source ouvert) assure la sécurité des conversations
- Dans Signal, il n'y a **aucune publicité, aucun vendeur partenaire, ni aucun système de suivi** inquiétant
- Signal est un organisme à **but non lucratif indépendant**. Ils ne sont reliés à aucune entreprise technologique importante et ils ne pourront jamais être achetés par l'une d'elles. Le développement de la plateforme est financé par des subventions et des dons.



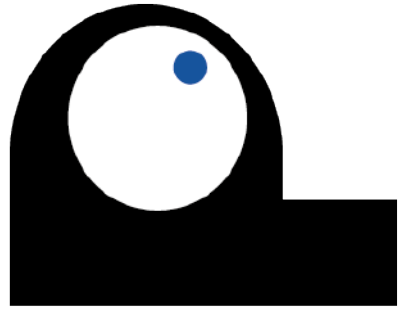
<https://signal.org/fr/download/>

ODILes

- ODILes vous permet d'échanger messages et documents en interne au sein de votre initiative pour coordonner votre équipe.
- Elle vous permet également de rejoindre des salons de discussion où vous retrouverez l'ensemble des initiatives d'ODIL.
- Un acteur malveillant ne pourra pas lire votre historique de messages, ni vos documents partagés *même si il dispose de votre mot de passe*. **Ces données sont chiffrées** grâce à votre clé de sécurité unique, ce qui offre un niveau de protection supplémentaire.



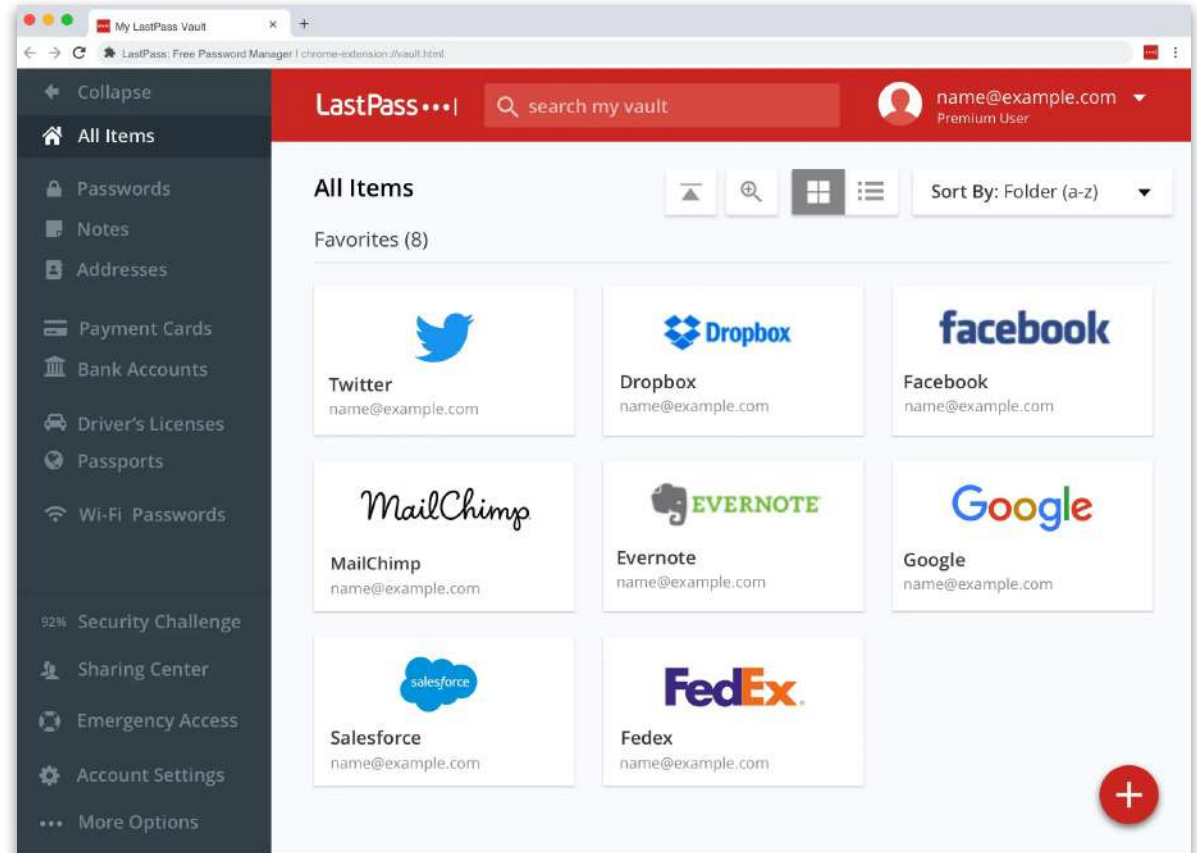
<https://play.google.com/store/apps/details?id=chat.idil.messaging>



GESTIONNAIRE DE
MOTS DE PASSE

GESTIONNAIRE DE MOTS DE PASSE

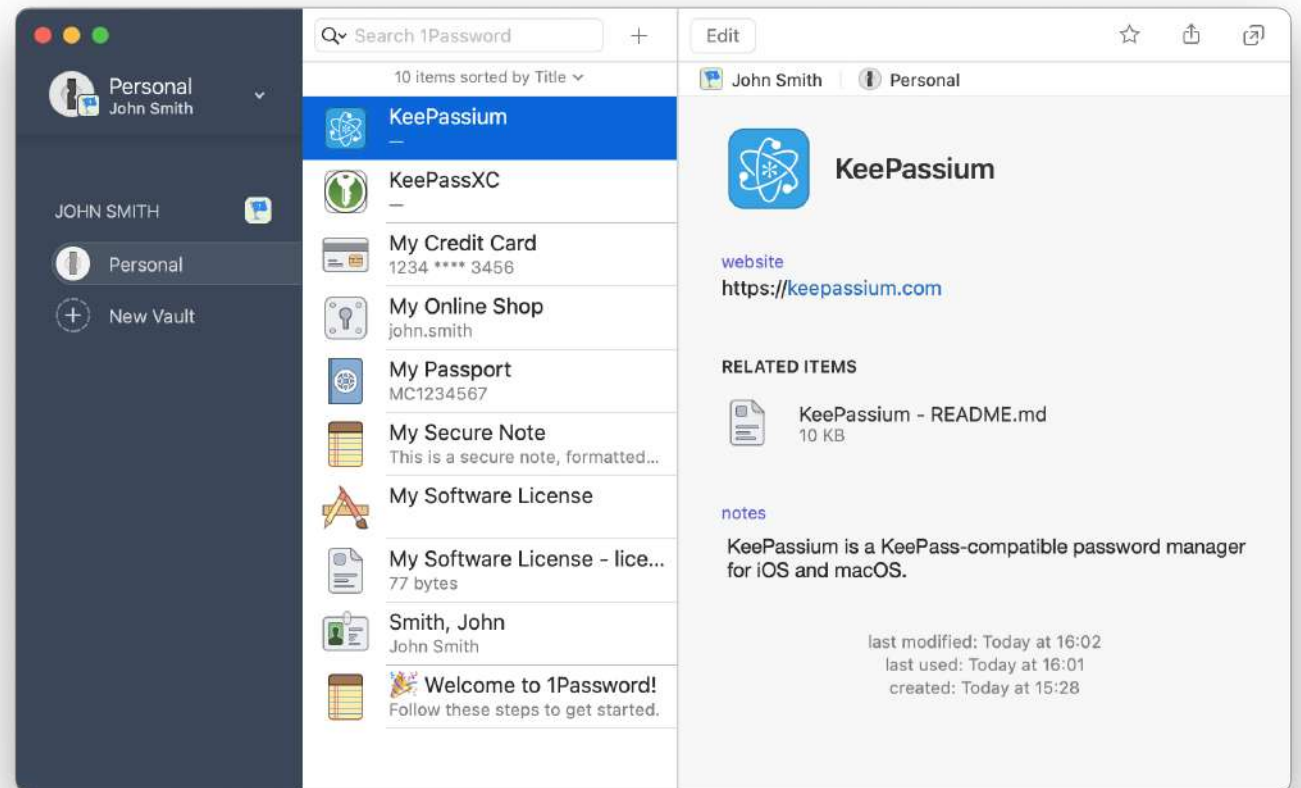
- Quand on crée un nouveau compte, un **mot de passe long et robuste** est requis. Sans ça, le compte ne peut être créé.
- Heureusement, **vous n'êtes pas obligé de vous souvenir de tous vos mots de passe**. Un gestionnaire de mots de passe s'en charge pour VOUS.



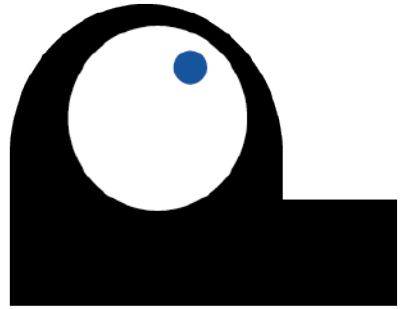
Source: [Wired](#)

PASSWORD MANAGER

- Les gestionnaires de mots de passe sont faits pour **stocker et gérer vos identifiants**.
- Ils **génèrent aussi des mots de passe robustes**. Ces mots de passe sont généralement stockés dans une base de données chiffrée et verrouillée par un mot de passe maître.
- Une fois que tous vos identifiants sont entrés dans la base de donnée, **le mot de passe maître est le seul dont vous devez vous rappeler**.
- Saisir votre mot de passe maître déverrouille la base de données et vous pouvez ensuite récupérer tous les identifiants qui s’y trouvent



Source: keepassium.com



APPLICATIONS

LASTPASS

Google Play Jeux Applications Films et TV Livres Enfants

LastPass Password Manager

GoTo Technologies USA, Inc.
Achats via l'appli

3.8★
225 k avis

10 M+
Téléchargements

Tout public

Installer

Bande-annonce

Store all of your passwords with LastPass.

And autofill those passwords for app and sites.

LastPass also creates strong, unique passwords for you.

Access your vault with your fingerprint.

And sync across unlimited devices.

Coordonnées du développeur

Applications similaires

1Password 8
AgileBits
3,6★

<https://play.google.com/store/apps/details?id=com.lastpass.lpandroid>

BITWARDEN

Google Play Games Apps Movies Books Kids

Quickly generate secure passwords

Length

7kMNuc9fuRWJvixBQiY9

Bitwarden Password Manager

Bitwarden Inc.

4.4★ 40.8K reviews

1M+ Downloads

Rated for 3+ Ⓔ

Install Add to wishlist

Trailer

Manage and store all of your passwords from an end-to-end encrypted Vault

Sync all of your passwords across multiple devices

Quickly generate secure passwords

Securely share passwords with your family, team, or entire company

Save time with autofill

Developer contact

Similar apps

1Password 8 - Password Manager
AgileBits
2.8★

<https://play.google.com/store/apps/details?id=com.x8bit.bitwarden>

1PASSWORD

Google Play Jeux Applications Films et TV Livres Enfants



1Password 8

AgileBits
Achats via l'app

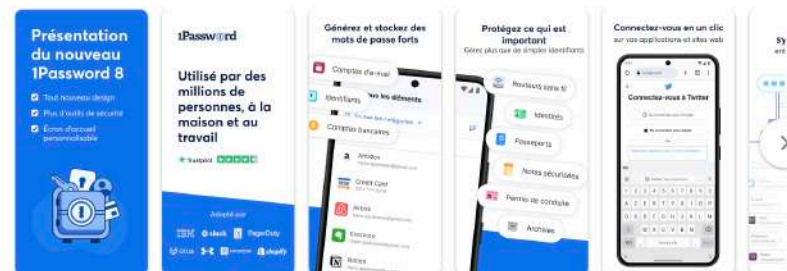
3,6★
3,38 k avis

500 k+
Téléchargements

Ⓔ
Tout public

Installer

Ajouter à la liste de souhaits



Coordonnées du développeur

Applications similaires

- One Key: password manager
GByte
4,7 ★
- AuthPass - Password Manager
CodeUX.design
4,1 ★
- Enpass password manager
Enpass Technologies Inc
4,1 ★
- DroidPass Password Manager
DroidApp BD
4,2 ★
- KPass: password manager

À propos de l'application

Des millions de particuliers et plus de 90 000 entreprises font confiance à 1Password pour garder leurs secrets en toute sécurité.

« Pour ceux qui veulent le meilleur gestionnaire de mots de passe pour leur téléphone, tablette et ordinateurs, 1Password est l'application à utiliser. »
—Android Central

Plus de sites à venir

<https://play.google.com/store/apps/details?id=com.onepassword.android>

1PASSWORD

Visite Familles Business Développeurs Prix Sécurité Télécharger Assistance Blog Connexion **Essayez GRATUITEMENT**

1Password pour le journalisme

Nous croyons en une presse libre et un Internet ouvert. Pour les journalistes qui travaillent dur pour atteindre cet objectif, nous voulons fournir les outils nécessaires pour rester en sécurité en ligne.

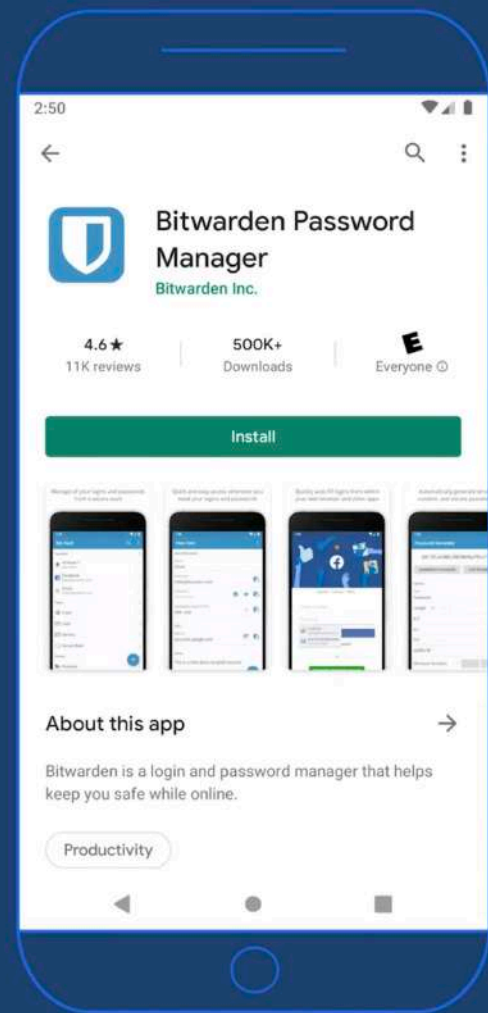
En partenariat avec

European Journalism Centre DataJournalism.com

Pour démarrer, entrez votre nom et votre email professionnel ci-dessous et créez un compte chez nous. Nous vous contacterons si nous avons besoin de toute information pour rendre votre compte complètement gratuit pour les journalistes individuels, ou un compte avec réduction pour les organisations de journalisme.

<https://1password.com/fr/for-journalism>

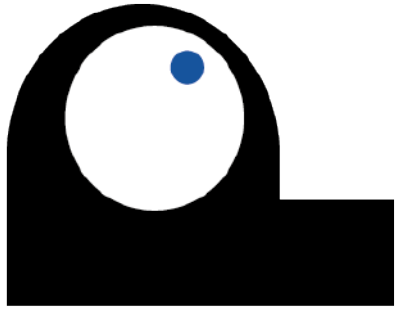
BITWARDEN



Bitwarden sur Android

Pour commencer avec Bitwarden sur Android, rechercher Bitwarden dans le Play Store

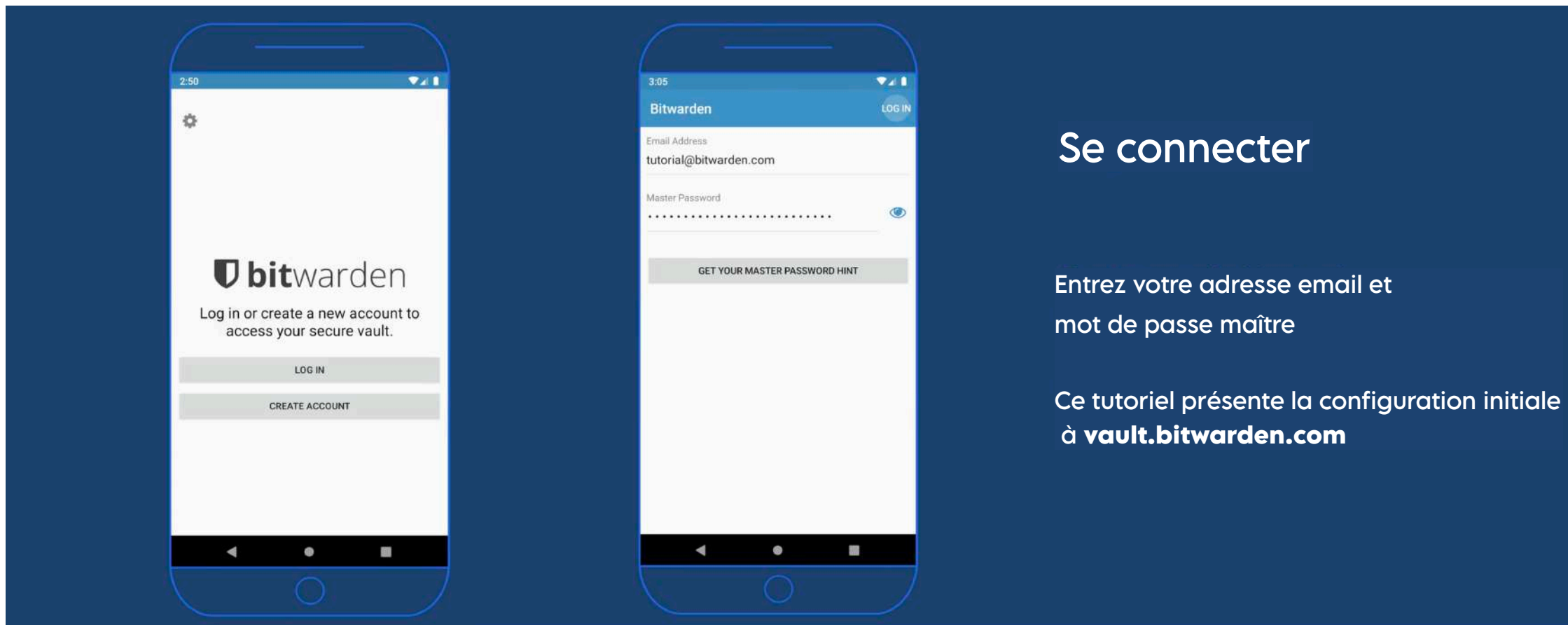
Ou se rendre sur get.bitwarden.com



SETUP

BITWARDEN

BITWARDEN

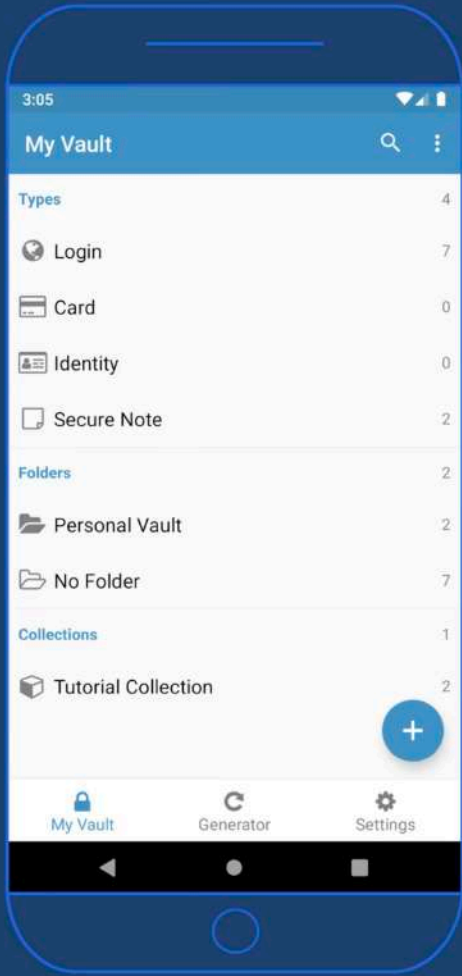


Se connecter

Entrez votre adresse email et
mot de passe maître

Ce tutoriel présente la configuration initiale
à **vault.bitwarden.com**

BITWARDEN



The screenshot shows the Bitwarden mobile app interface. At the top, the status bar displays the time 3:05 and signal strength. The app title 'My Vault' is at the top left, with a search icon and a menu icon to its right. Below the title, there are three main sections: 'Types', 'Folders', and 'Collections'. Each section lists items with their respective counts. A blue plus sign button is located at the bottom right of the main content area. At the bottom, there is a navigation bar with three icons: 'My Vault', 'Generator', and 'Settings'.

Category	Item	Count
Types	Login	7
	Card	0
	Identity	0
	Secure Note	2
	Total	4
Folders	Personal Vault	2
	No Folder	7
	Total	2
Collections	Tutorial Collection	2
	Total	1

Bienvenue dans votre coffre

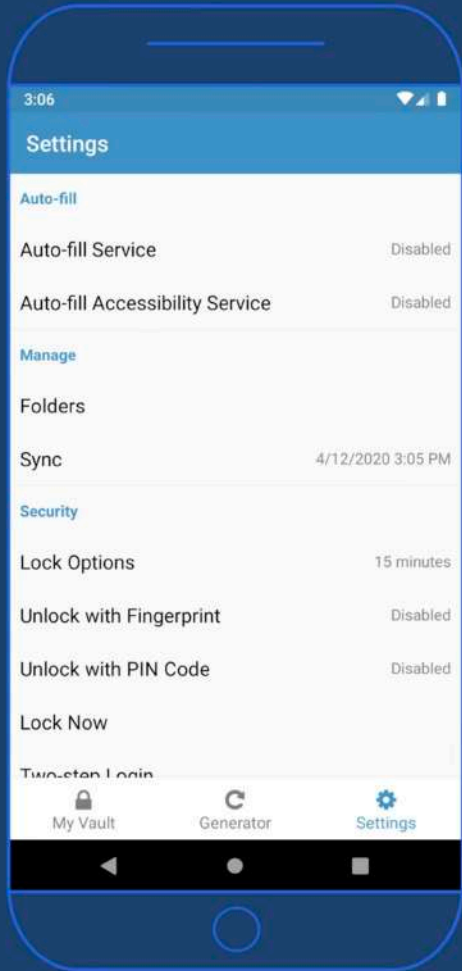
Vos informations sécurisées

- Identifiants, cartes, identités, notes sécurisées

Des **dossiers** pour vos effets personnels

Des **collections** pour les effets partagés

BITWARDEN AJOUTER UN IDENTIFIANT

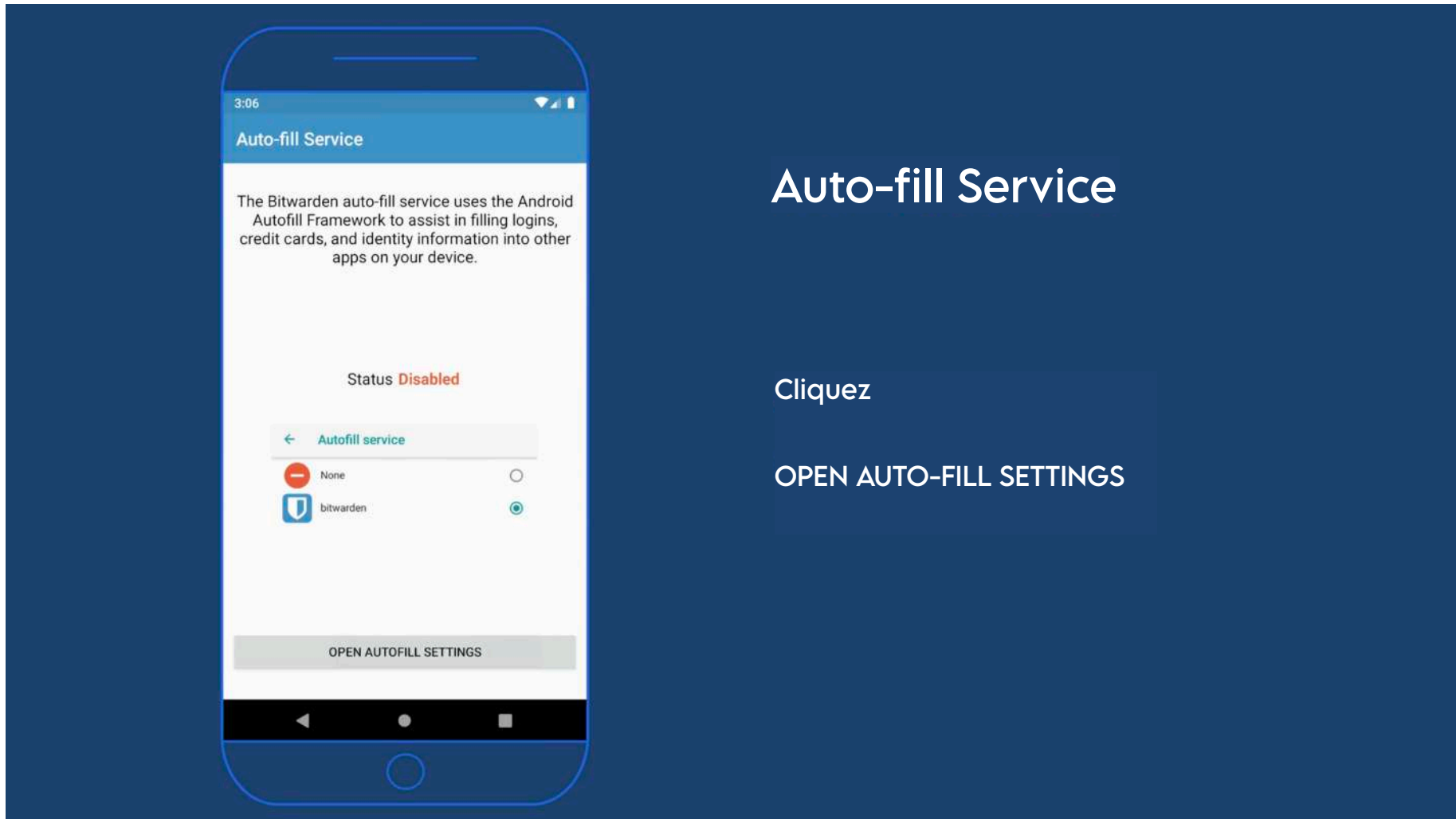


Fonctionnalités Auto-fill

Nous conseillons d'activer les deux options

Activons d'abord **Auto-fill Service**

BITWARDEN AJOUTER UN IDENTIFIANT

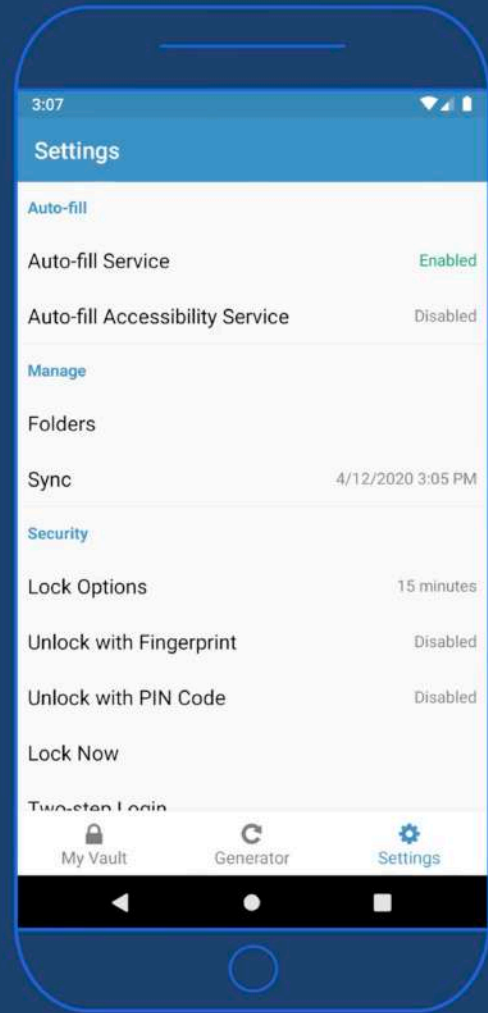


Auto-fill Service

Cliquez

OPEN AUTO-FILL SETTINGS

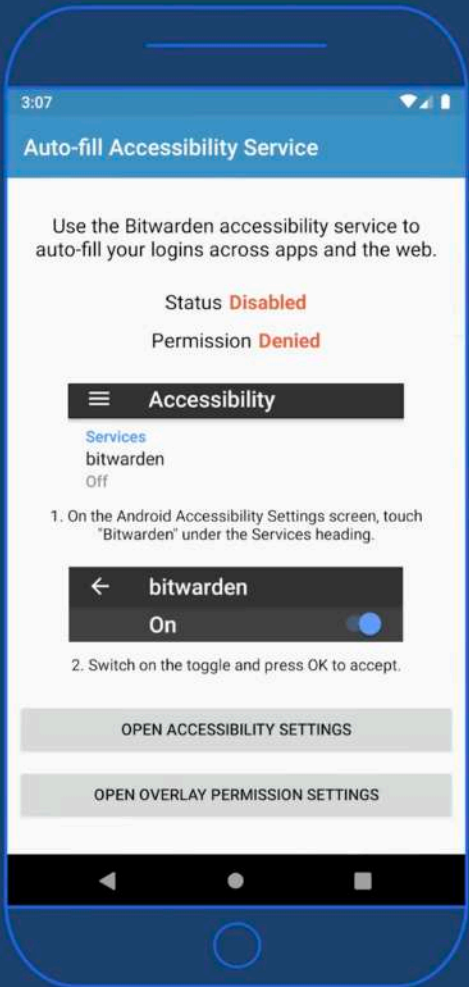
BITWARDEN AJOUTER UN IDENTIFIANT



Auto-fill Accessibility Service

Ensuite, activez le
Auto-fill Accessibility Service

BITWARDEN AJOUTER UN IDENTIFIANT



Auto-fill Accessibility Service

Use the Bitwarden accessibility service to auto-fill your logins across apps and the web.

Status **Disabled**

Permission **Denied**

Accessibility

Services

bitwarden
Off

1. On the Android Accessibility Settings screen, touch "Bitwarden" under the Services heading.

bitwarden
On

2. Switch on the toggle and press OK to accept.

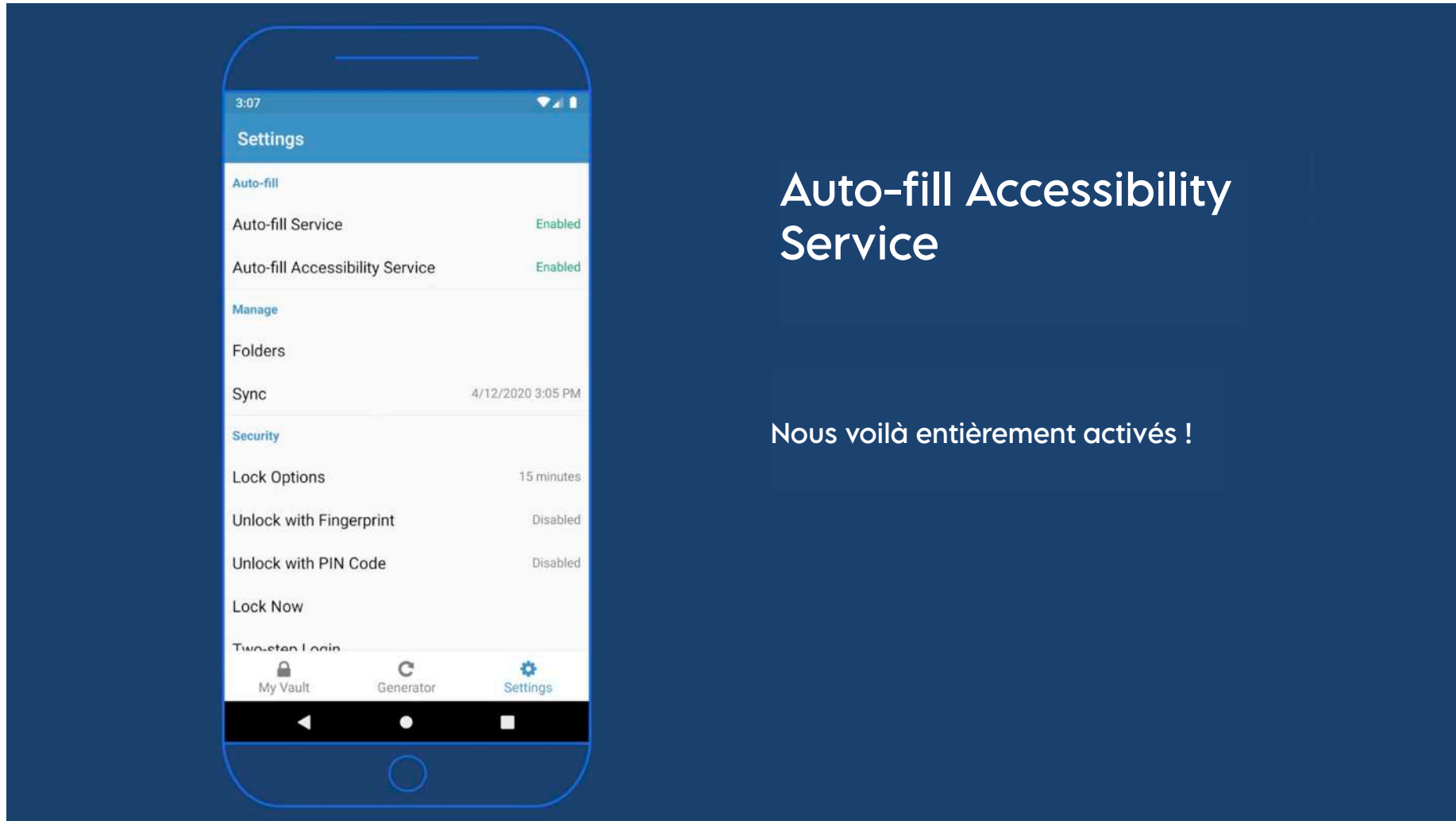
OPEN ACCESSIBILITY SETTINGS

OPEN OVERLAY PERMISSION SETTINGS

Auto-fill Accessibility Service

Cliquez d'abord sur
OPEN ACCESSIBILITY SETTINGS

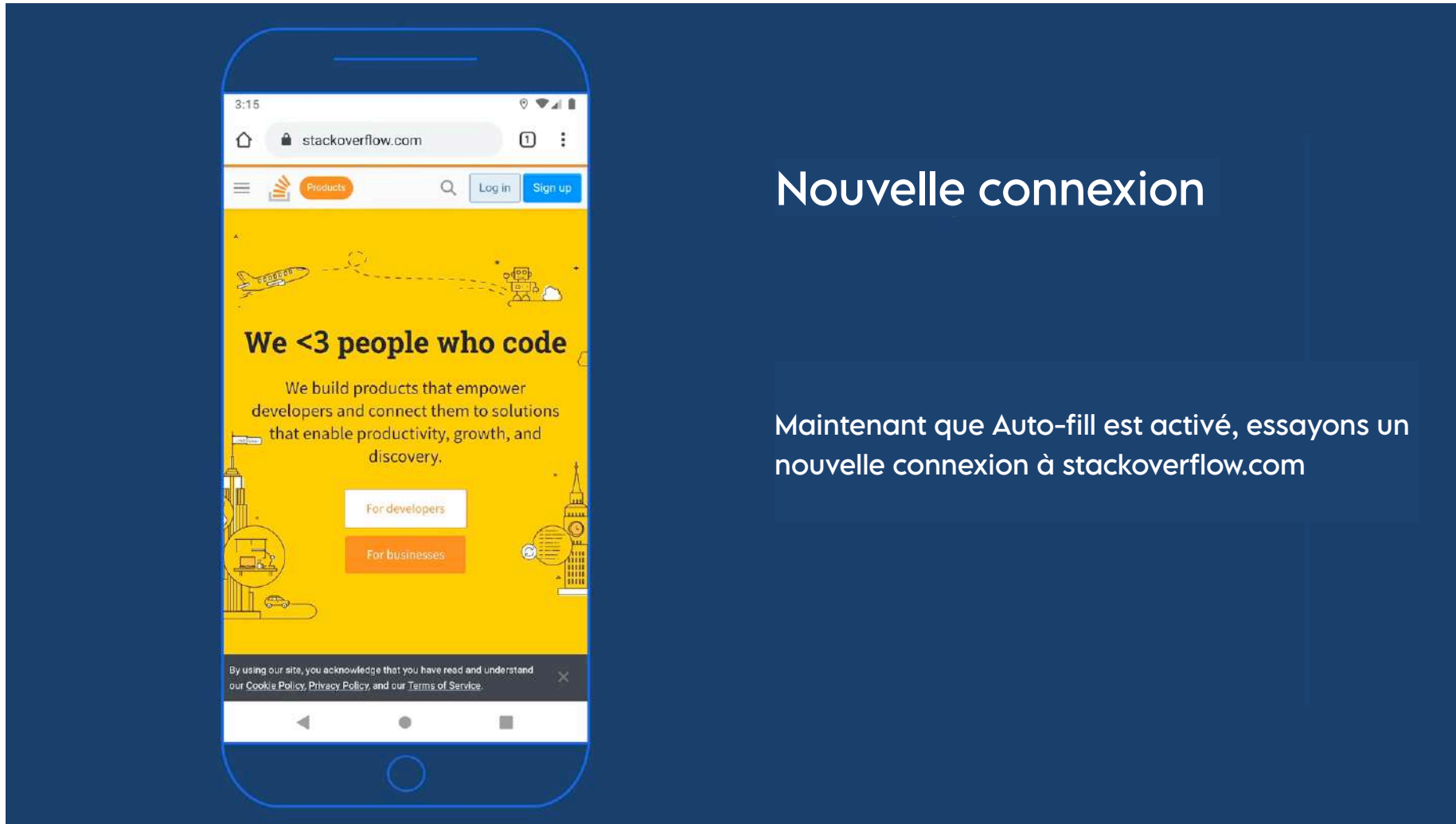
BITWARDEN AJOUTER UN IDENTIFIANT



Auto-fill Accessibility Service

Nous voilà entièrement activés !

BITWARDEN CONNEXION

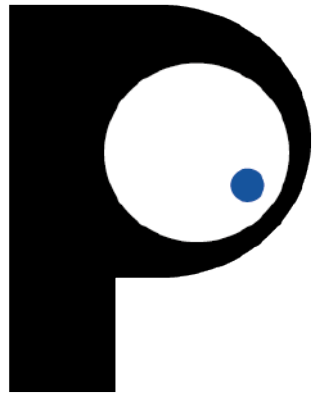


Nouvelle connexion

Maintenant que Auto-fill est activé, essayons un nouvelle connexion à stackoverflow.com

BITWARDEN CONNEXION





AUTHENTIFICATION
À DEUX FACTEURS (2FA)

AUTHENTIFICATION À DEUX

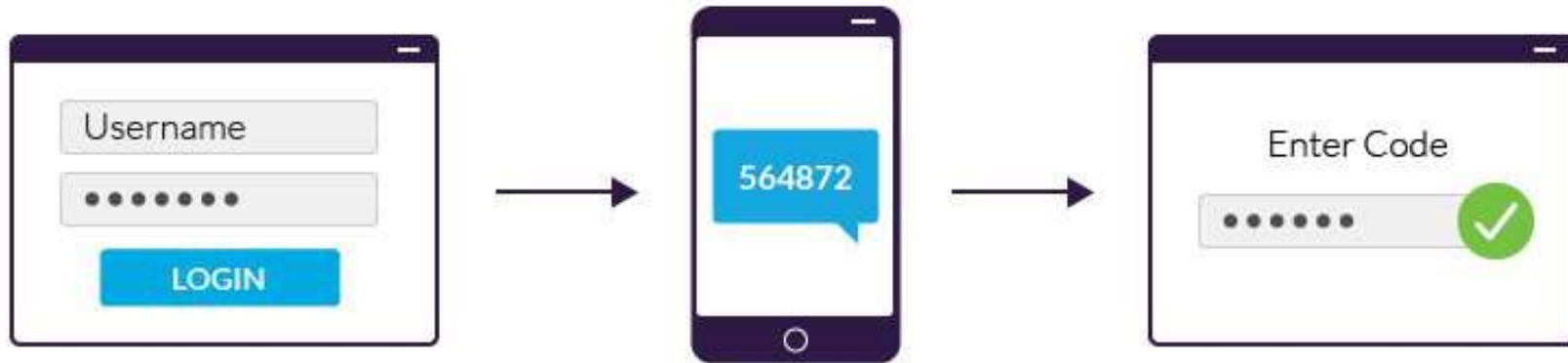
FACTEURS

- Quand vous créez un compte sur un site ou une application, on vous demande un **identifiant** ou un **email**, ainsi qu'un **mot de passe**.
- L'authentification à deux facteurs consiste à **renforcer la protection** de vos comptes en **ajoutant une deuxième couche d'authentification** :
 - envoyer un code unique par SMS
 - envoyer un code valide pour une durée limitée (TOTP)
 - utiliser un code avec validation sur un autre appareil
 - utiliser une application d'authentification
 - utiliser la reconnaissance faciale, de la voix ou des empreintes digitales
 - utiliser une clé de chiffrement ou une clé de sécurité



Source: [lemagit.fr](https://www.lemagit.fr)

AUTHENTIFICATION À DEUX FACTEURS



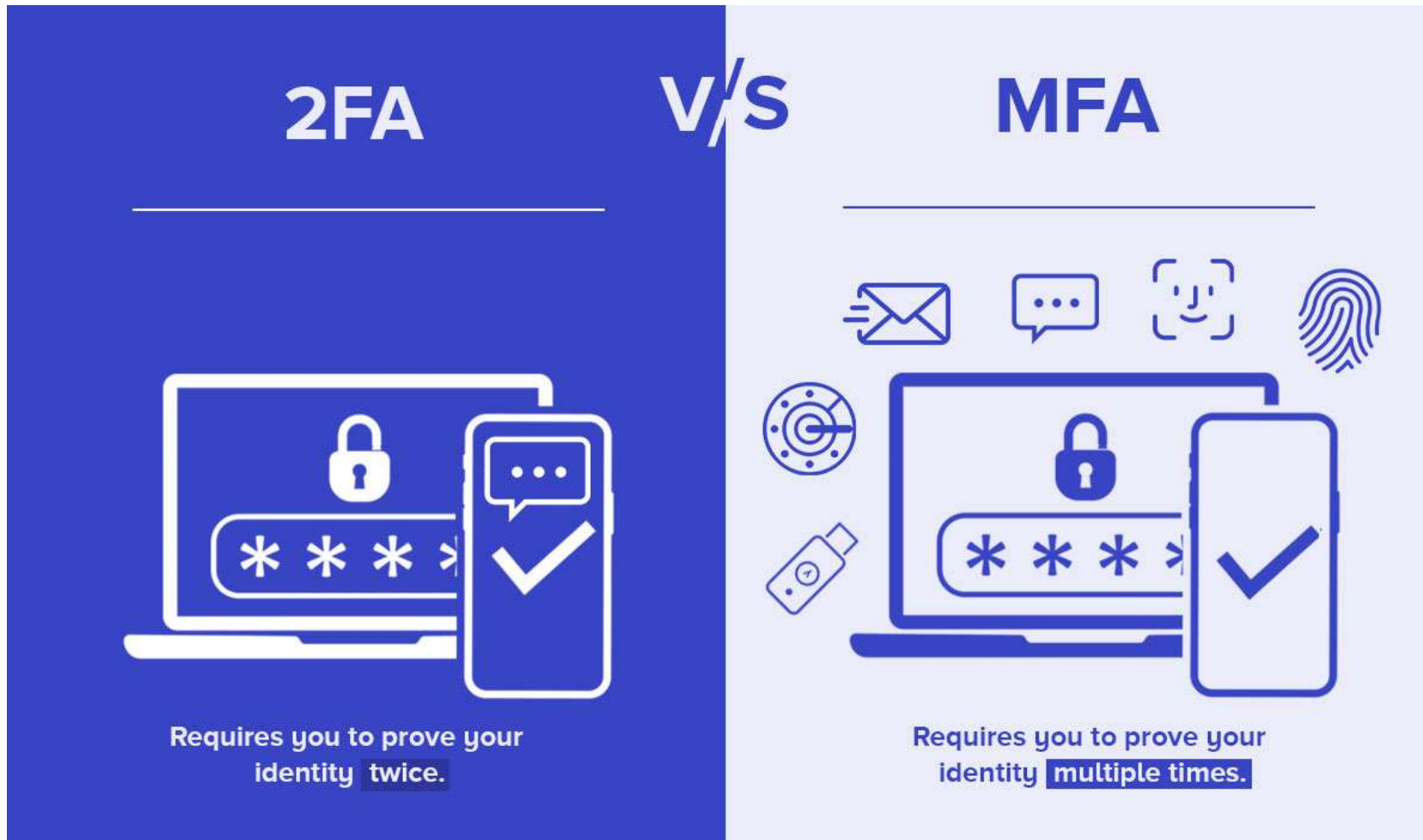
L'utilisateur entre son identifiant et mot de passe

Un code d'authentification est envoyé à l'appareil mobile de l'utilisateur

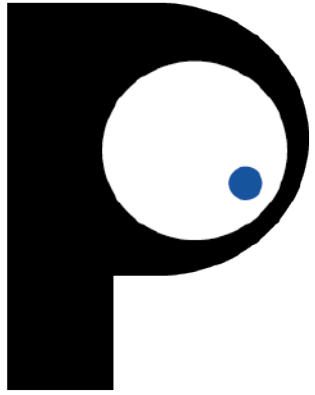
L'utilisateur entre son code d'authentification pour se connecter à l'application

Source: funinformatique.com

2FA VS MFA



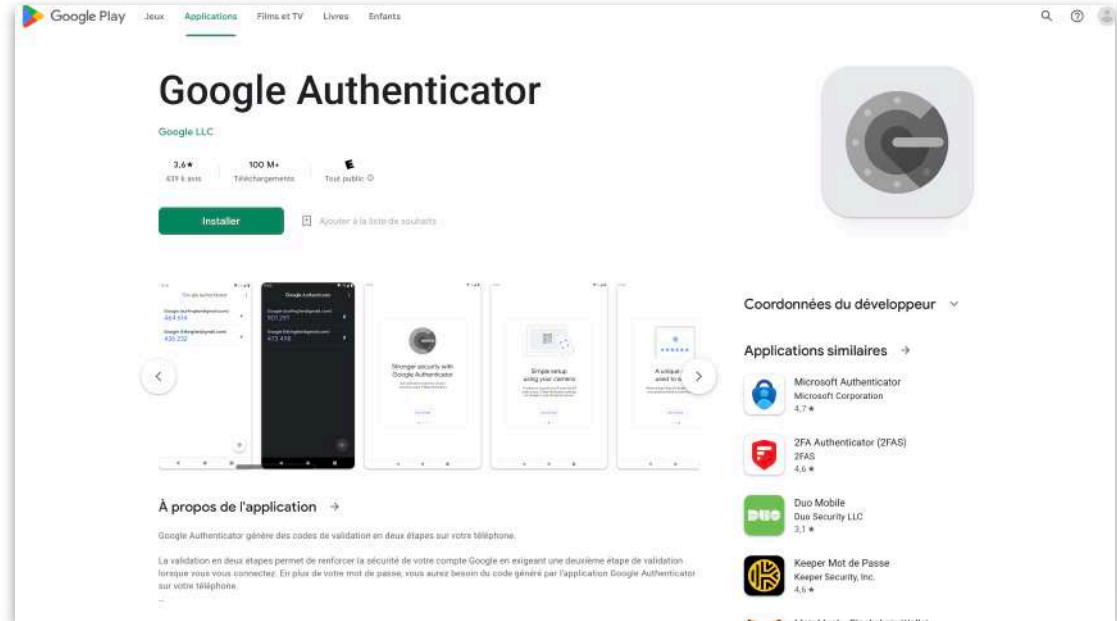
Source: quicklaunch.io



APPLICATIONS

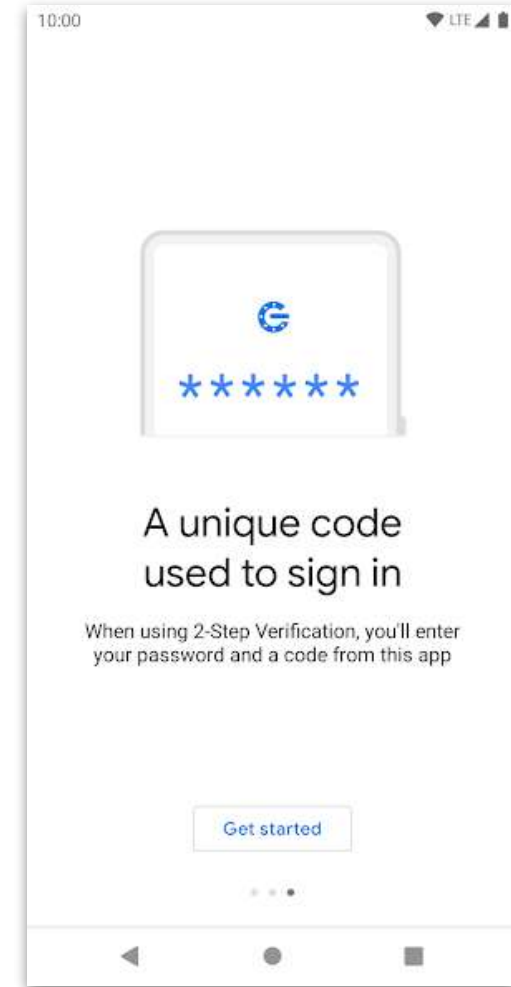
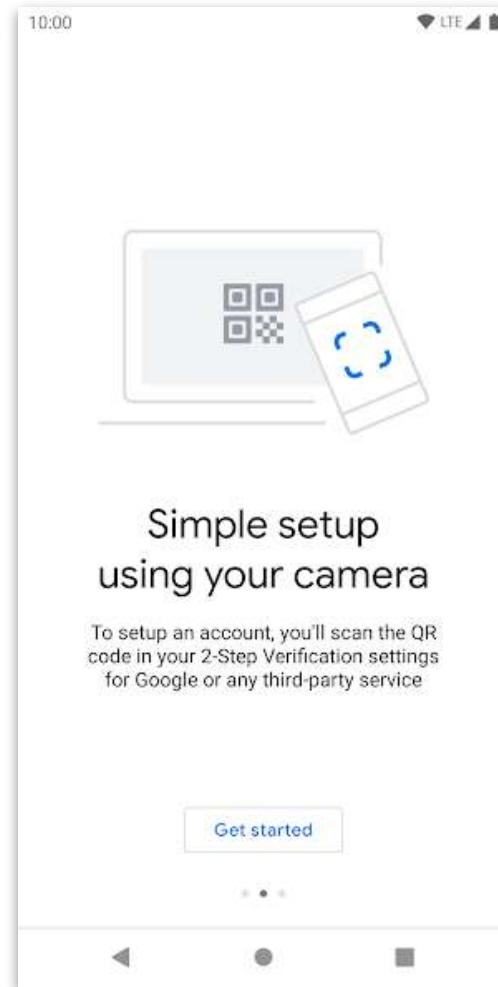
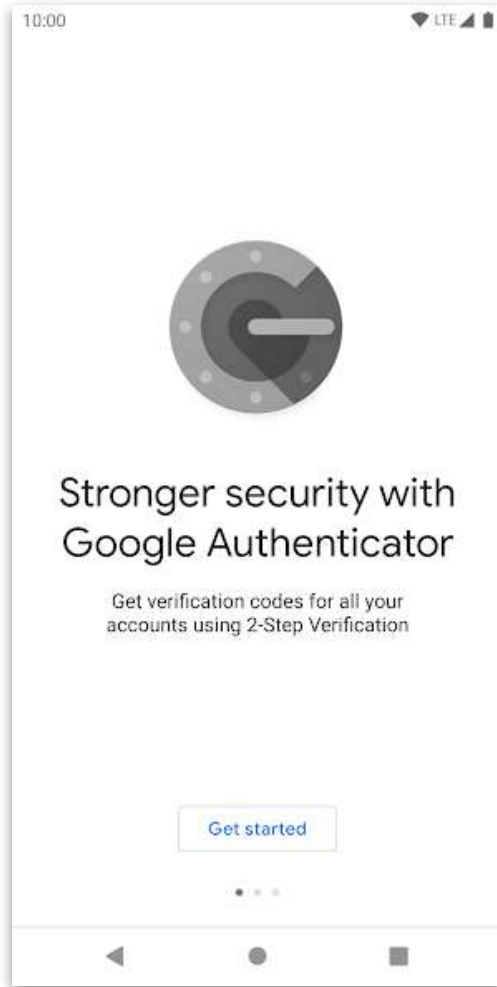
GOOGLE AUTHENTICATOR

Google Authenticator est un logiciel d'authentification qui implémente le service de vérification en deux étapes grâce à l'algorithme **Time-based One-time Password (TOTP)** et à l'algorithme **HMAC-based One-time Password (HOTP)**, pour authentifier les utilisateurs d'applications logicielles.



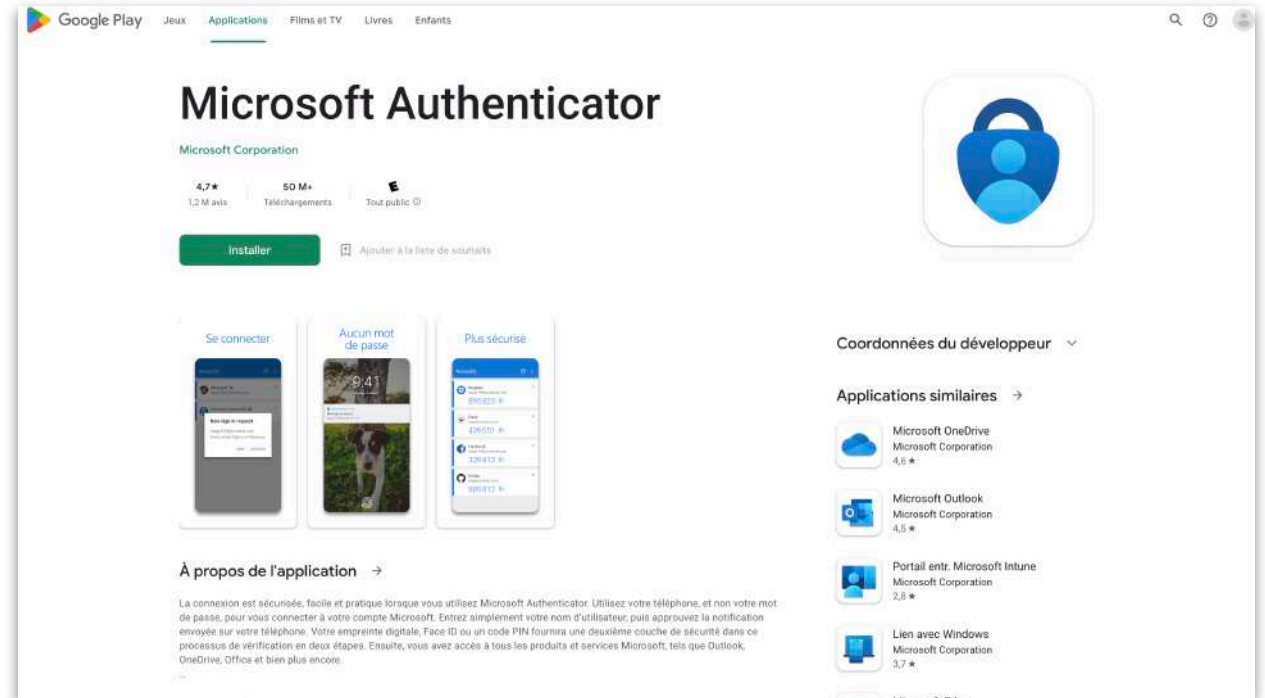
<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2>

GOOGLE AUTHENTICATOR



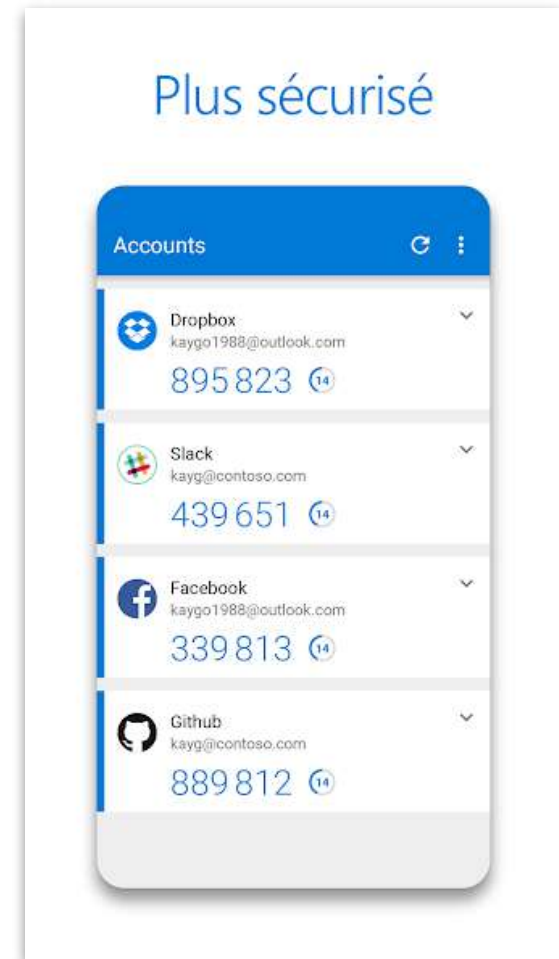
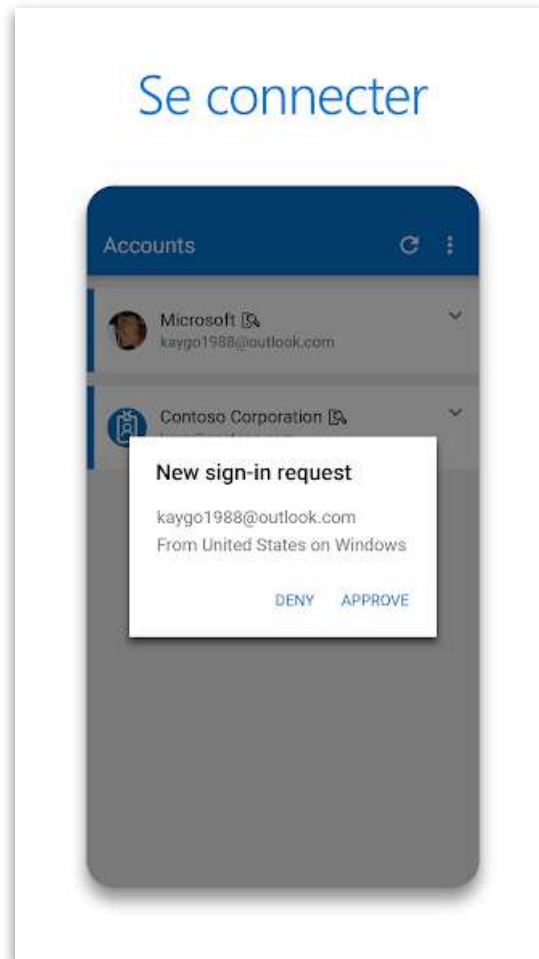
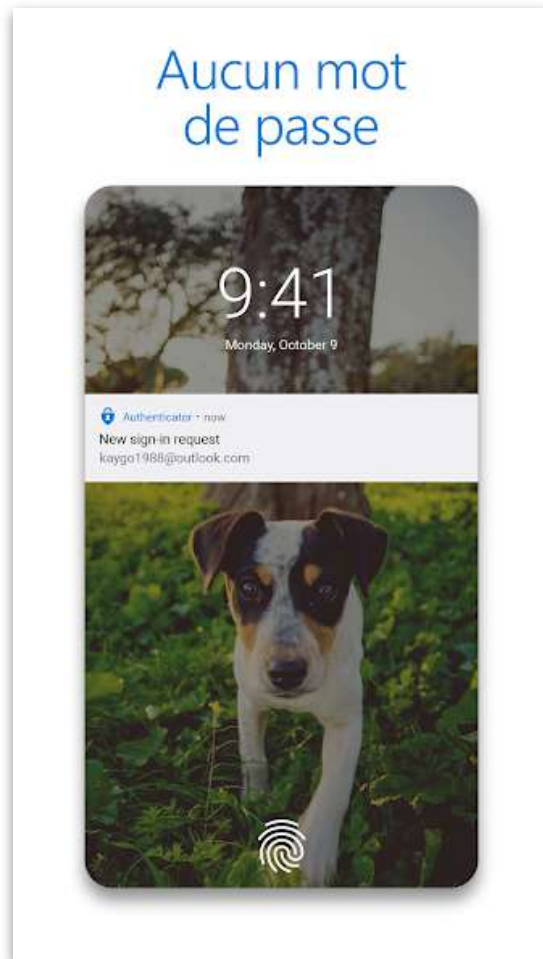
MICROSOFT AUTHENTICATOR

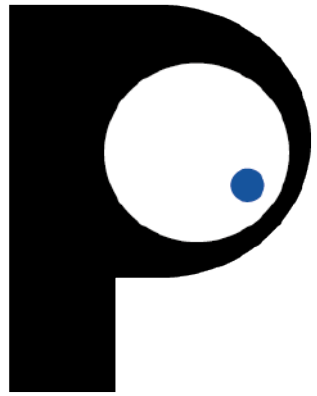
- Entrez votre identifiant
- Ensuite, acceptez les notifications envoyées à votre téléphone. Vos empreintes digitales, la reconnaissance faciale ou un PIN procurent une deuxième couche de sécurité dans cette authentification à deux facteurs.



<https://play.google.com/store/apps/details?id=com.azure.authenticator>

MICROSOFT AUTHENTICATOR

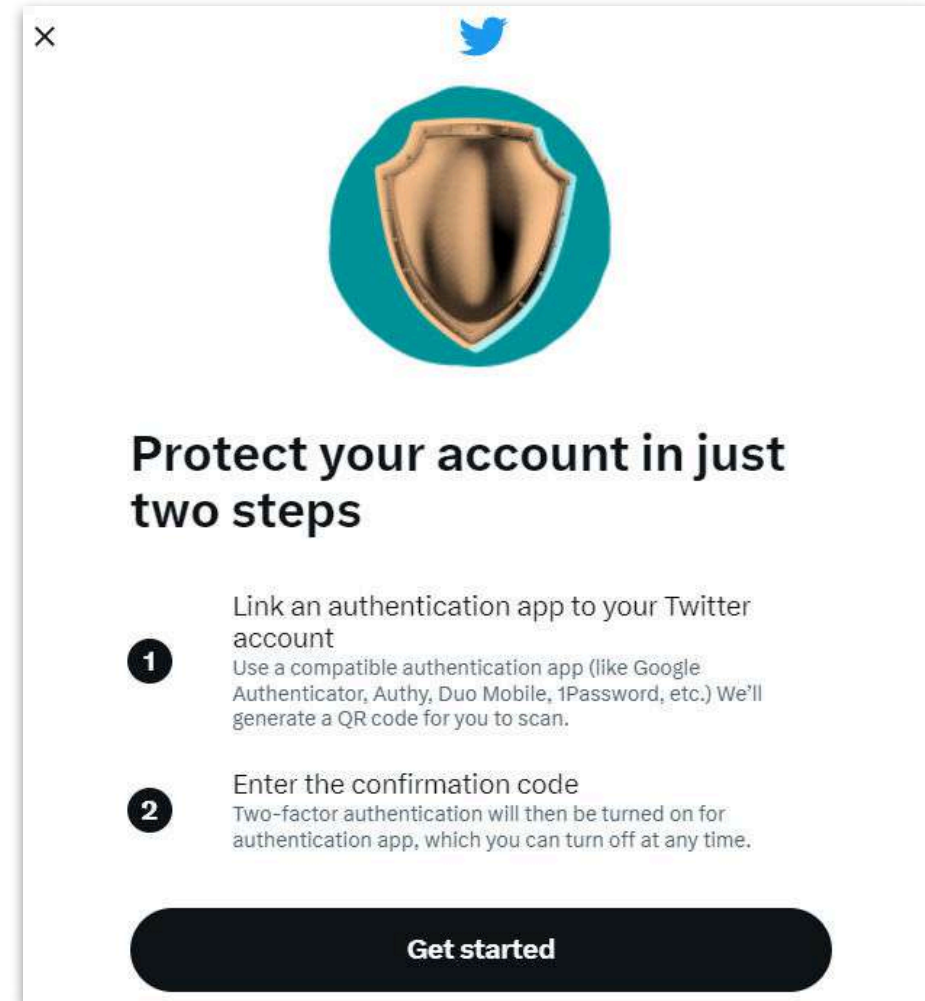




INSTALLER 2FA
POUR TWITTER

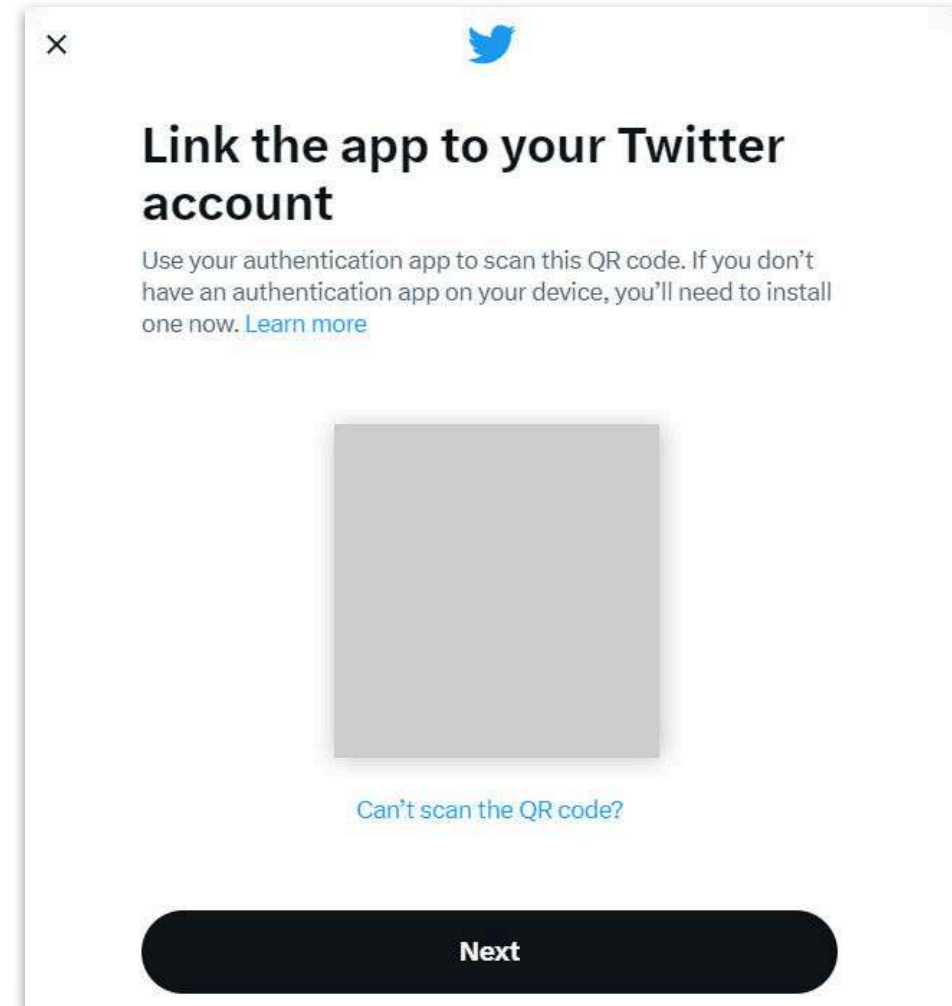
INSTALLER 2FA POUR TWITTER

1. En étant connecté, allez sur **Réglages et support** > **Réglages et confidentialité** > **Sécurité et accès au compte** > **Sécurité** > **Authentification à deux facteurs**
2. Cliquez **Application d'authentification** et entrez votre mot de passe. Cliquez le bouton **Commencer**.



INSTALLER 2FA POUR TWITTER

3. Vous verrez ensuite un QR code sur la page **Connecter l'application à votre compte Twitter.** Ouvrir votre application d'authentification et cliquez l'option **Scanner un QR code.**
4. Pointez votre téléphone vers l'écran et le code sera scanné automatiquement. Si ce n'est pas le cas, votre application vous demandera de faire cette étape manuellement. Cliquez **Suivant.**



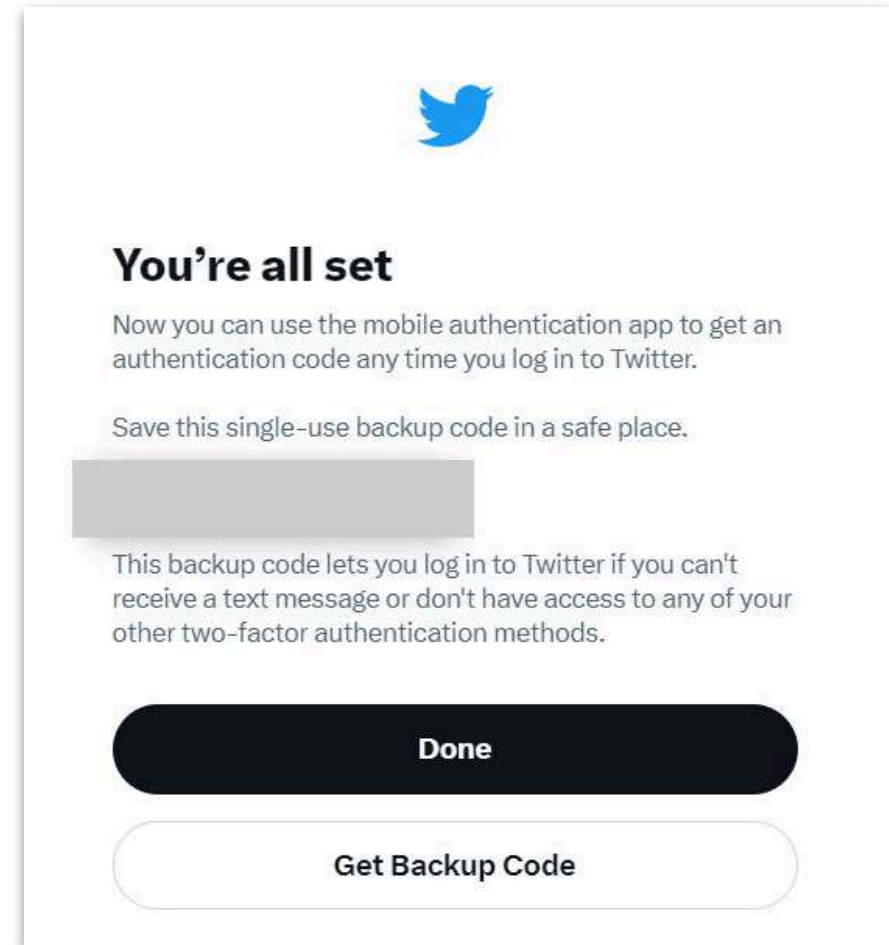
INSTALLER 2FA POUR TWITTER

5. Si l'étape précédente a marché, vous verrez un code à 6 chiffres généré par Twitter pour votre application d'authentification.

6. Entrez le code dans la popup sur Twitter afin de connecter votre compte.

Si le code change avant que vous l'ayez entré, pas d'inquiétude, entrez simplement le nouveau code.

Notez-vous votre code de récupération, il peut être utilisé pour vous connecter si vous perdez vos appareils ou l'accès à vos méthodes d'authentification.





@fs0c131y



baptiste@predictalab.com

