Guide Utilisateur Cyberfiltre Mobile et Cyberfiltre Mobile Avancé

Cyberfiltre Mobile

Comment personnaliser mon service Cyberfiltre Mobile

Depuis le menu **“Tableau de bord” du portail Cyberfiltre Mobile**, vous pouvez vérifier la protection de votre ligne et la configurer à votre guise et selon vos besoins.

Entre autres options, vous pouvez créer des profils pour personnaliser la protection de vos appareils, consulter l'historique des blocages de votre ligne, vérifier si vos comptes Internet ont été exposés à des cyberattaques et vérifier si une page Web est potentiellement malveillante.

Ci-dessous, nous allons décrire la configuration de ces options étape par étape, et vous pouvez également consulter la video suivante pour découvrir les différentes fonctionnalités :

Statut de votre protection

Dès que vous ouvrirez la page de personnalisation de votre ligne, vous pourrez vérifier si vous êtes protégé, ou si vous avez des actions en cours (veuillez consulter la rubrique « **Vérification d'identité** »).

Gestion des profils

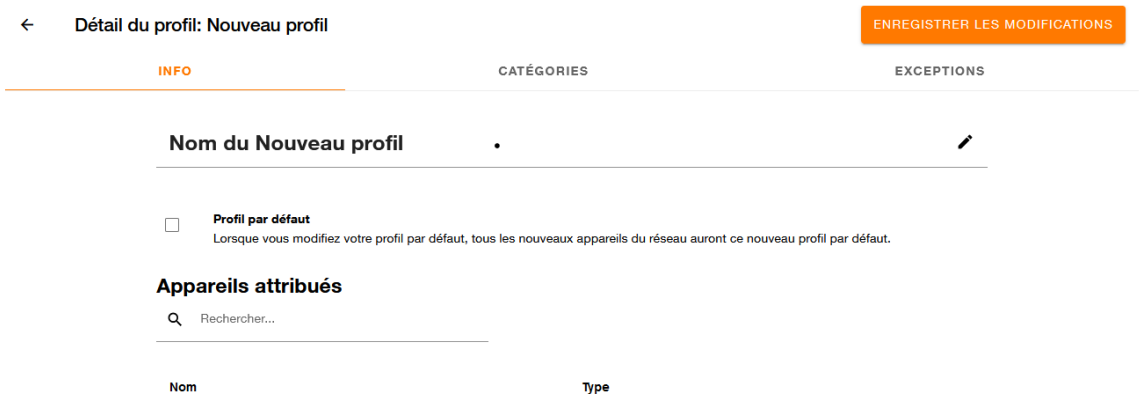
Dans la rubrique «**profils** », vous pouvez créer et modifier des profils afin de personnaliser votre protection :

Comment puis-je créer un nouveau profil ?

Dans la rubrique « **profils** », vous pouvez modifier le profil par défaut déjà créé et appliqué à votre ligne mobile. Vous pouvez également créer autant de nouveaux profils que vous le souhaitez pour vos lignes et appareils.

Pour cela, cliquez simplement sur le bouton « + », option « **ajouter un profil** » et donnez un nom au profil que vous souhaitez créer..

AJOUTER UN NOUVEAU PROFIL

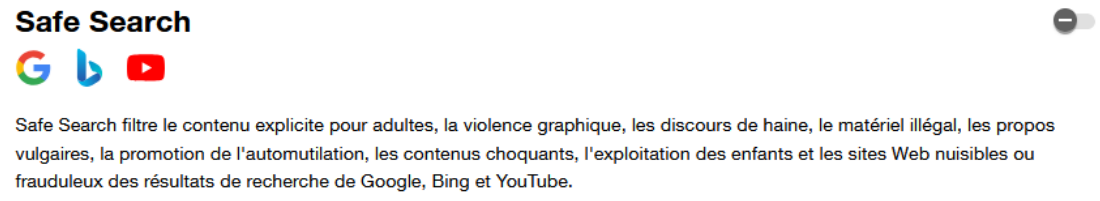


N'oubliez pas d'enregistrer les modifications

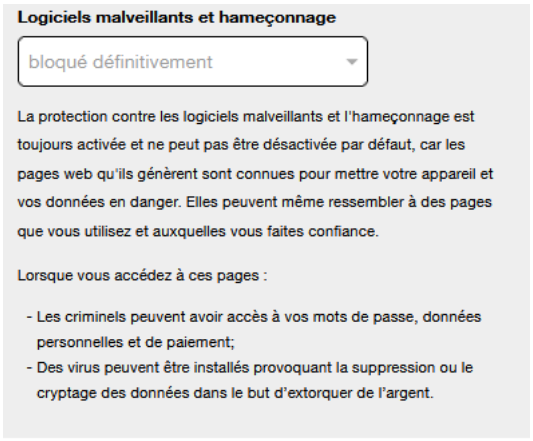
ENREGISTRER LES MODIFICATIONS

Quelles options de protection dois-je personnaliser dans mes profils ?

Dans vos profils, vous pouvez configurer des filtres de contenu Web pour décider quelles catégories Web vous souhaitez autoriser et lesquelles vous ne souhaitez pas autoriser.



En plus de bloquer par défaut les sites Web de phishing et de logiciels malveillants,



vous pouvez décider si vous souhaitez bloquer les catégories de sites Web suivantes :

- Pornographie
- Pari
- Violences
- Drogue
- Site de streaming
- Réseaux sociaux

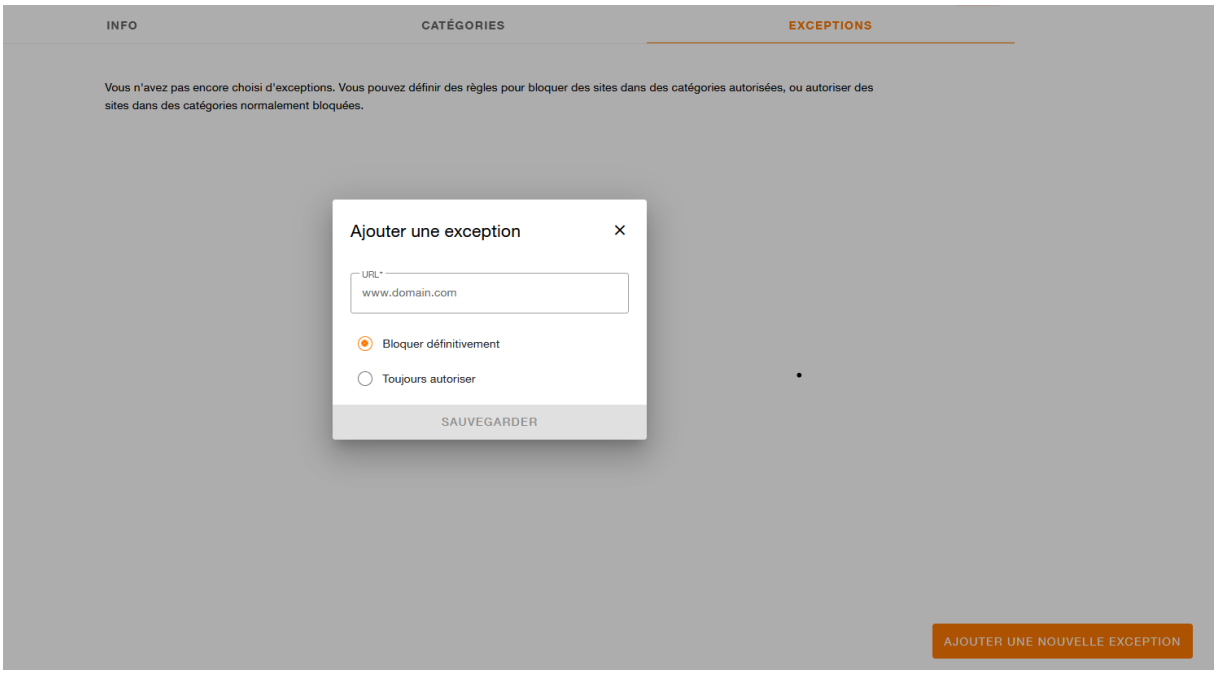
N'oubliez pas d'enregistrer vos modifications afin qu'elles soient appliquées.

Puis-je définir des exceptions ?

Oui, même si vous bloquez une certaine catégorie, vous pouvez inclure les exceptions que vous souhaitez autoriser ou interdire.

Allez simplement dans la section « **Exceptions** », et cliquez sur le bouton « **+** » pour ajouter une exception.

Saisissez l'adresse Web que vous souhaitez configurer comme exception et n'oubliez pas d'enregistrer les modifications.



Puis-je bloquer d'autres catégories ou adresses Web ?

Il n'y a plus de catégories Web configurées sur votre service que vous puissiez bloquer.

Cependant, si vous souhaitez bloquer une adresse Web spécifique sans qu'elle n'appartienne à l'une des catégories configurées, vous pouvez le faire à titre exceptionnel.

Ajoutez simplement une exception et définissez-la sur « **bloquer définitivement** » afin que ladite adresse Web soit bloquée, qu'elle appartienne ou non à l'une des catégories disponibles.

Si je bloque une catégorie Web, les applications mobiles correspondantes sont-elles également bloquées ?

Non, en bloquant les catégories Web, les applications pouvant correspondre à ces catégories ne sont pas bloquées (comme par exemple : les applications de réseaux sociaux). Vous pourrez toujours accéder à vos reseaux sociaux via les apps installées sur l'appareil.

Cependant, il est possible que de nombreuses fonctionnalités de ces applications dont vous avez bloqué la catégorie soient désormais inutilisables, puisque la navigation Web qu'elles utilisent sera également bloquée.

Mais **Cyberfiltre Mobile** ne peut pas garantir que l'utilisation de l'application soit complètement désactivée, car certaines fonctionnalités peuvent continuer à fonctionner, comme la messagerie par exemple.

À quelles lignes et appareils chaque profil s'applique-t-il ?

Dans la section « **Informations** » de chaque profil est indiqué à quelle ligne et à quels appareils s'applique la configuration du profil.

Sans aucune intervention de votre part, les paramètres de protection de votre ligne mobile (réseau 4G/ 5G) sont appliqués au profil « **Par défaut** ». Si vous souhaitez qu'ils s'appliquent à un nouveau profil que vous avez créé, n'oubliez pas de définir ce profil par défaut.

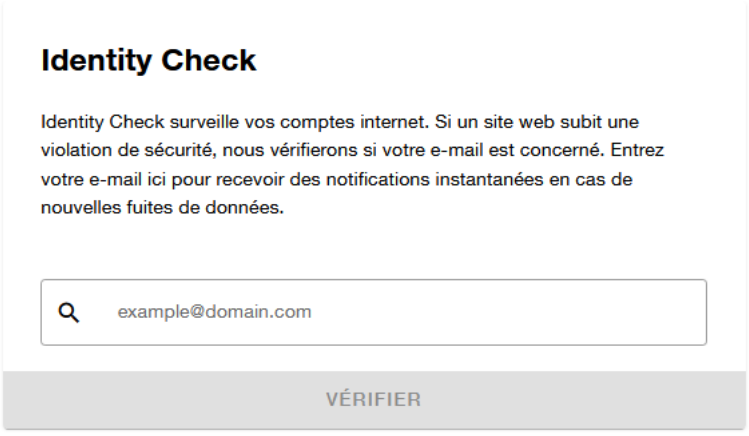
Pour chaque nouvel appareil sur lequel vous téléchargez les applications, vous pouvez choisir les paramètres de profil que vous souhaitez appliquer. Pour plus d'informations, veuillez consulter les articles suivants relatifs à la gestion des appareils.

Gérer les appareils

Dans la section « **Gérer les appareils** », vous pouvez ajouter et gérer des appareils sur lesquels télécharger vos applications **Cyberfiltre Mobile Avancé Réunion / Mayotte**. Veuillez consulter les sections de téléchargement d'applications suivantes pour plus d'informations.

Vérification d'identité

Dans l'option « **Vérification d'identité** », vous pouvez vérifier si vos comptes Internet ont été exposés à une cyberattaque ou à une fuite de vos données personnelles.



Quelles sont les fuites de mes comptes internet ?

Les sites Web sur lesquels vous utilisez votre courrier électronique comme compte de connexion peuvent être exposés à des cyberattaques et à des violations de données. Cela

signifie que vos données personnelles ou autres données confidentielles associées, peuvent avoir été compromises (par exemple : vos mots de passe) et être disponibles sur Internet.

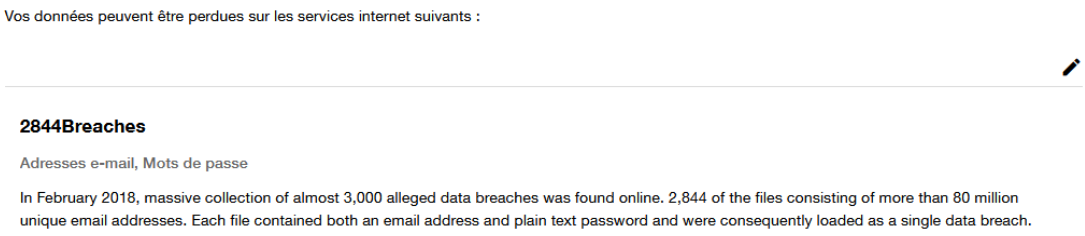
Comment puis-je vérifier si mes comptes de messagerie ont été exposés ?

Entrez simplement votre email et cliquez sur « **Vérifier** ».

Si vous êtes victime d'une fuite d'adresse email, une liste de sites internet sur lesquels ce risque a pu exister s'affichera. Nous vous recommandons de modifier votre mot de passe sur ces sites Internet pour empêcher un éventuel accès à vos données personnelles.

J'ai déjà modifié mon mot de passe sur les sites Web exposés, pourquoi sont-ils toujours répertoriés ?

Orange Cyberfiltre Mobile détecte les fuites sur les sites internet qui utilisent votre email comme compte de connexion. Si vous avez déjà modifié votre mot de passe, vous pouvez supprimer les sites Web en cliquant sur le « crayon » et en sélectionnant les sites Web à supprimer de la liste.



Si j'enregistre mon adresse e-mail, saurai-je quand une violation s'est produite ?

Oui, si vous enregistrez votre email, Cyberfiltre Mobile vous avertira dans la rubrique « **Quelque chose doit être fait** » si une nouvelle fuite s'est produite, afin que vous puissiez modifier le mot de passe sur le site internet concerné.

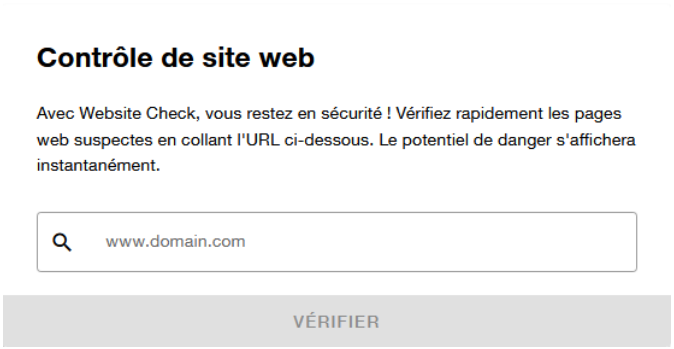
Puis-je empêcher la fuite de mon adresse e-mail ?

Il n'est pas possible de l'éviter. Mais vous pouvez prendre certaines mesures pour améliorer votre sécurité, comme changer périodiquement vos mots de passe ou demander la suppression des comptes que vous n'utilisez plus.

Vérifier un site Web

Dans la rubrique « **Contrôle de site Web** », vous pouvez vérifier toute adresse Web dangereuse. Copiez et collez simplement l'adresse Web et cliquez sur « **Vérifier** ».

Cyberfiltre Mobile vous indiquera si ladite adresse web est potentiellement dangereuse ou frauduleuse, sans que vous ayez à y accéder.



Pourquoi devriez-vous vérifier si un site Web est sécurisé ?

Si vous n'êtes pas sûr qu'un site Web soit faux ou dangereux, vous pouvez vérifier ce site Web avant de le visiter avec votre navigateur. De cette façon, vous éviterez tout risque éventuel.

Que dois-je faire si Cyberfiltre Mobile m'informe que le site web n'est pas sécurisé ?

Ne visitez pas ce site Web avec votre navigateur, sinon vos données pourraient être en danger !

Cyberfiltre Mobile Avancé

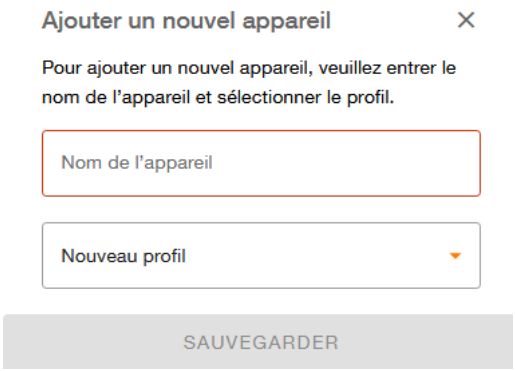
C'est très simple, ci-dessous nous vous expliquons en détail les étapes à suivre pour télécharger, installer et utiliser votre application Cyberfiltre Mobile Avancé.

Téléchargez l'application « Cyberfiltre Mobile Reunion / Mayotte »

Pour commencer le processus de téléchargement de l'application de protection Wifi & Antivirus « **Cyberfiltre Mobile Avancé** », vous devez accéder à votre espace de

1. Depuis le menu de gestion de votre service Cyberfiltre Mobile, disponible dans votre espace client
2. Vous accéderez directement à la section « Gérer les appareils » depuis la page Tableau de bord.

3. Sélectionnez « **Ajouter un nouvel appareil** » et donnez un nom à l'appareil sur lequel vous allez télécharger l'application (il peut s'agir du même appareil via lequel vous accédez à ce menu ou d'un appareil différent). Vous devez également associer l'un des profils créés à cet appareil ajouté.



4. Ensuite, un code d'activation sera généré (également disponible sous forme de QR code), dont vous aurez besoin pour vous authentifier pendant le processus d'installation de l'application.

5. Cliquez sur le logo Apple Store ou Google Play, ou si vous envisagez d'installer l'application sur un autre appareil que celui utilisé pour la configuration, accédez au store des applications de votre appareil, recherchez « Cyberfiltre Mobile Reunion Mayotte » Application d'Orange et démarrez le processus d'installation.

Questions liées au téléchargement :

Pourquoi un appareil apparaît-il déjà avec mon numéro de téléphone ?

Cet enregistrement identifie votre ligne mobile et la protection associée, c'est pourquoi elle appraît identifiée avec votre numéro de téléphone.

Puis-je télécharger l'application sur n'importe quel appareil ?

Oui, vous pouvez télécharger l'application **Cyberfiltre Mobile** sur n'importe quel appareil mobile. n'est pas nécessaire qu'il s'agisse du même appareil avec lequel vous avez accédé au menu de téléchargement. Vous aurez simplement besoin du code d'activation pour pouvoir poursuivre l'installation sur l'appareil sur lequel vous avez décidé de télécharger l'App.

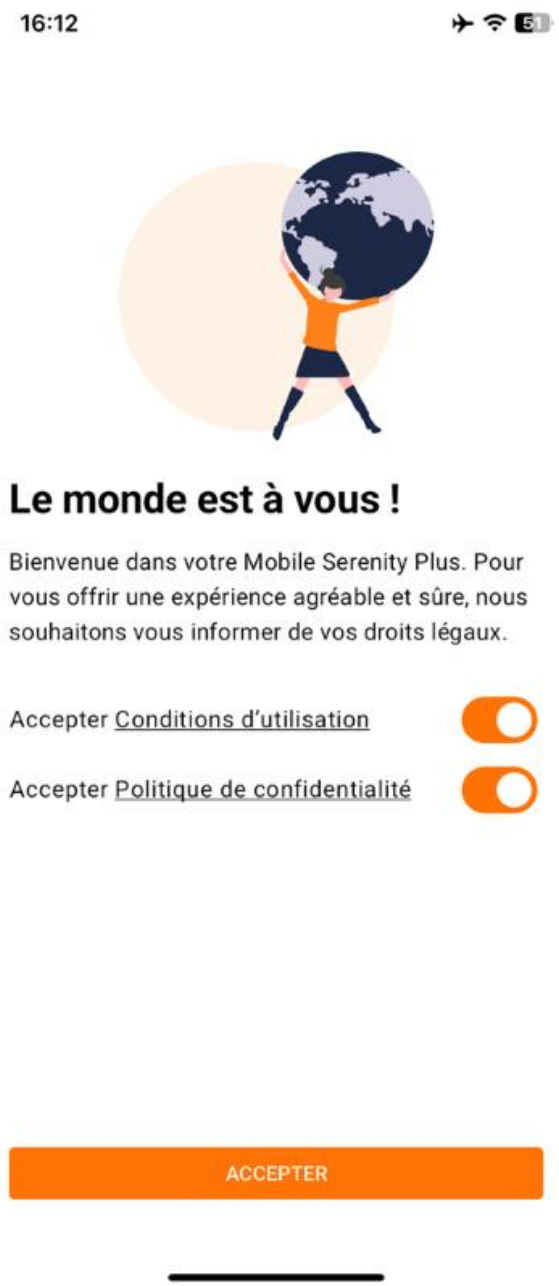
Sur combien d'appareils puis-je télécharger l'application Cyberfiltre Mobile Avancé ?

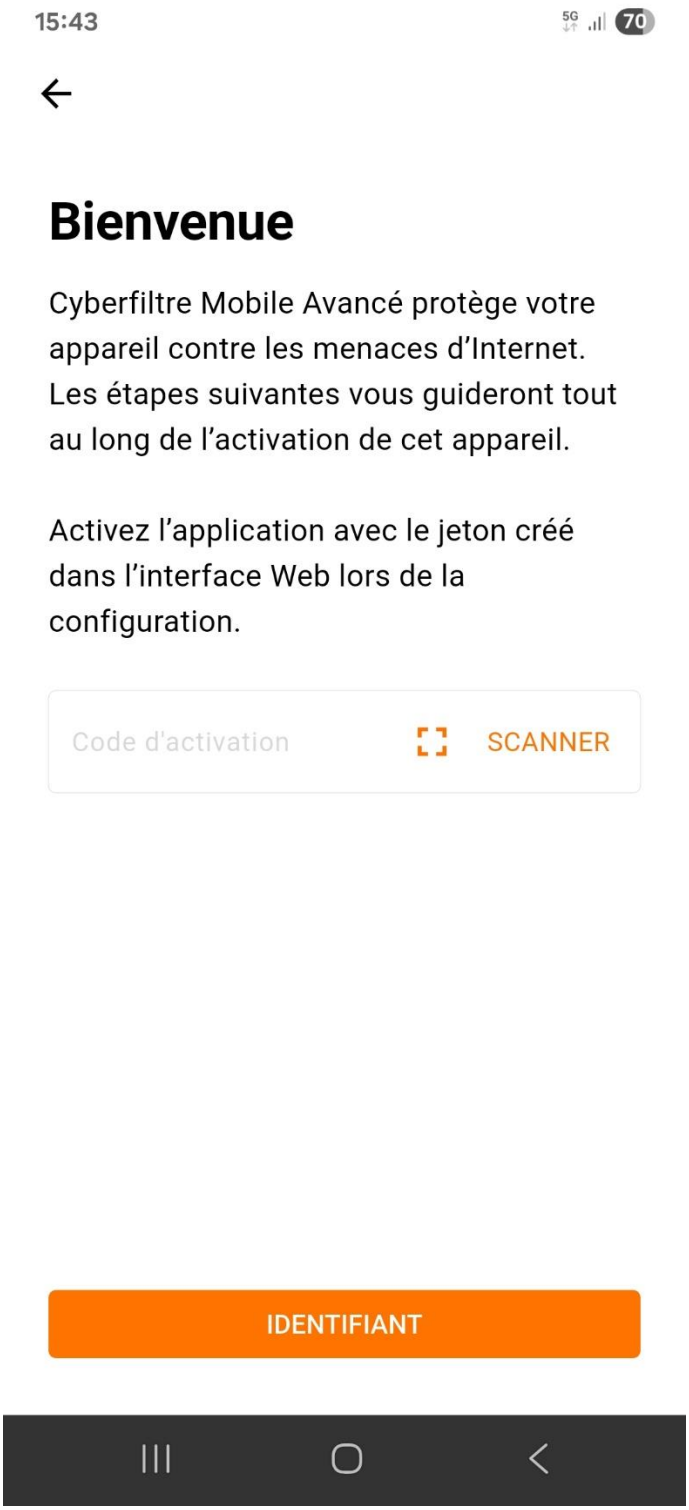
Vous pouvez télécharger l'application Cyberfiltre Mobile Avancé sur chaque appareil dont l'abonnement mobile dispose de l'option de protection.

Installez l'application de protection Wifi & Antivirus Cyberfiltre Mobile Avancé

Une fois que vous avez téléchargé et démarré l'installation de votre l'application de protection Wifi & Antivirus **Cyberfiltre Mobile Avancé vous devez accepter les « Conditions d'utilisation »** et la « **Politique de confidentialité** ».

Ensuite, sur l'écran suivant du processus d'installation, vous devez saisir le code d'activation. Vous pouvez le faire en le copiant et en le collant si vous souhaitez installer l'application sur le même appareil sur lequel vous l'avez généré, ou en scannant le code QR si vous souhaitez installer l'application sur un autre appareil.





Pendant le processus d'installation, veuillez accepter les autorisations demandées par l'application pour « **Lire le stockage externe** », « **Gérer le stockage externe** », et autorisez également l'application à établir une connexion **VPN (Secure Connection)**.

Voilà, vous avez bien installé l'application !

Questions liées à l'installation :

Puis-je installer l'application sans accepter toutes ces autorisations ?

Non, pour que l'application s'installe et fonctionne correctement, vous devez accepter toutes les autorisations demandées lors du processus d'installation.

Existe-t-il une autre application susceptible d'être incompatible avec l'application Cyberfiltre Mobile Avancé ?

Oui, si une application liée à AddBlocker, VPN ou iCloud Private Relay d'Apple est installée sur votre appareil, votre application de cyberprotection ne fonctionnera pas correctement. Veuillez désactiver ou désinstaller ces applications afin que l'application **Cyberfiltre Mobile Avancé** fonctionne correctement.

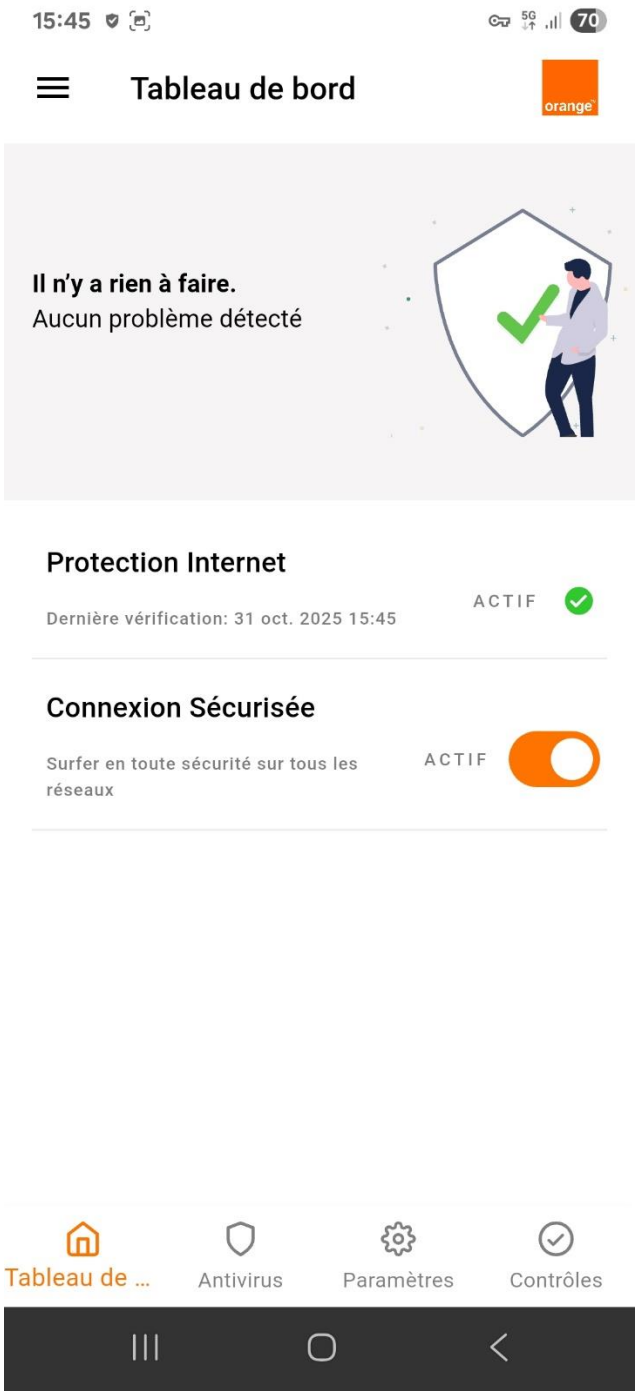
Est-il possible de ne pas être protégé par Cyberfiltre Mobile Avancé lorsque j'utilise un VPN alternatif ?

Tant que vous utilisez un VPN autre que **Cyberfiltre Mobile Avancé**, vous ne serez pas protégé ! Chaque fois qu'un autre VPN est utilisé, tout le trafic est acheminé via cet autre VPN, ce qui rend techniquement impossible l'analyse de la cyber protection et donc votre protection contre les contenus nuisibles.

Questions liées au fonctionnalités de l'application Cyberfiltre Mobile Avancé

Tableau de bord

Dans le menu principal de l'application **Cyberfiltre Mobile Avancé**, vous pouvez vérifier l'état de votre Connexion Sécurisée (VPN), ainsi que l'historique des sites Web bloqués par l'application.



L'option Connexion Sécurisée n'est pas active, que dois-je faire ?

Si l'option Connexion Sécurisée n'est pas active, vous ne serez pas protégé.

Parfois, après avoir redémarré votre appareil ou que votre appareil a été redémarré lors d'une mise à jour, l'option Connexion Sécurisée peut avoir été désactivée. Ouvrez l'application et vérifiez que votre connexion sécurisée VPN est activée. Sinon, rallumez-le.

Après avoir redémarré mon appareil, le VPN ne se réactive pas automatiquement. Que puis-je faire?

Lors de l'installation de l'application, vous deviez autoriser votre appareil pour que la connexion VPN soit toujours active. Si vous l'avez ignoré et n'avez pas activé cette fonctionnalité dans les paramètres de votre appareil, la connexion sécurisée VPN risque de ne pas redémarrer après le redémarrage de votre appareil.

Veuillez accéder aux paramètres de votre appareil et activer l'option Always On VPN.

Puis-je désactiver la connexion sécurisée VPN quand je le souhaite ?

Bien sûr, vous pouvez désactiver manuellement la connexion sécurisée VPN à tout moment, mais rappelez-vous que si vous faites cela, vous ne serez plus protégé.

Menu antivirus (Android uniquement) :

Grâce à la fonctionnalité Antivirus, vous pouvez vérifier si votre appareil contient des fichiers ou des applications dangereux ou frauduleux. Appuyez simplement sur « **Démarrer l'analyse** » et attendez la fin de celle-ci. Si à la suite de ce scan, **Cyberfiltre Mobile Avancé** détecte un fichier dangereux, l'application vous l'indiquera et vous donnera la possibilité de le supprimer de votre appareil.

Est-ce dangereux si je ne supprime pas les fichiers détectés par l'antivirus de mon appareil ?

Oui, si l'option antivirus identifie une application ou un fichier comme infecté, il est dangereux de ne pas le supprimer, vos données personnelles pourraient être en danger !

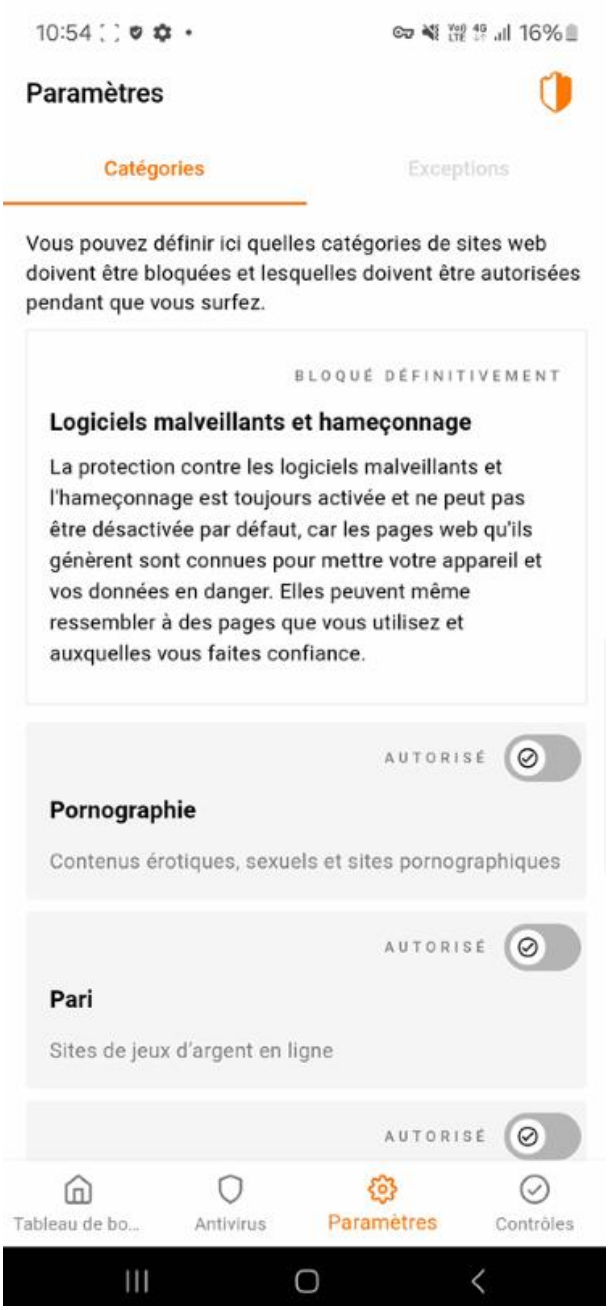
Dois-je effectuer des analyses périodiques de mon appareil ?

Oui, il est recommandé d'analyser périodiquement votre appareil pour détecter d'éventuels applications ou fichiers dangereux.

Mon appareil est un iPhone, pourquoi ne puis-je pas trouver l'option antivirus ?

En raison des limitations inhérentes au système d'exploitation iOS, l'option antivirus n'est malheureusement pas disponible pour les appareils iPhone. Par conséquent, vous ne pourrez utiliser cette fonctionnalité que si votre appareil est Android.

Menu Paramètres :



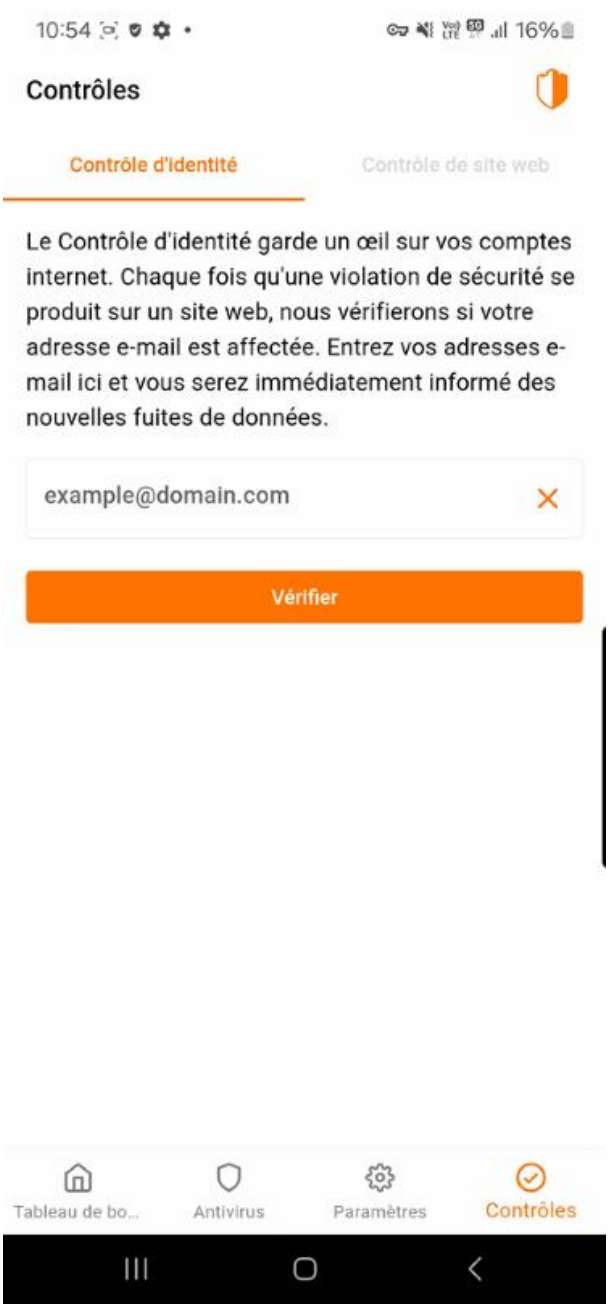
Dans le menu **Paramètres**, vous pouvez modifier les filtres de contenu Web pour décider quelles catégories Web vous souhaitez autoriser l'accès et pour lesquelles vous ne souhaitez pas le faire.

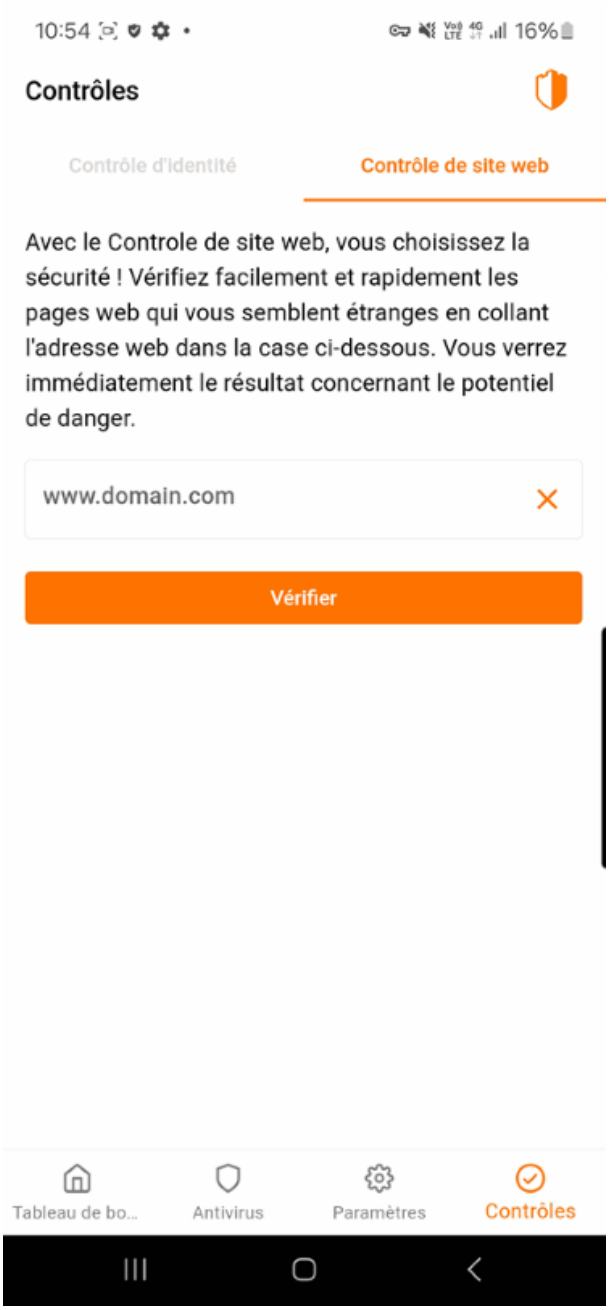
N'oubliez pas qu'en plus de bloquer par défaut les sites Web de phishing et de logiciels malveillants, vous pouvez décider si vous souhaitez bloquer les catégories de sites Web suivantes, depuis le menu « **Gérer les profils** » dans votre portail Cyberfiltre Mobile.

- Pornographie
- Pari
- Violence
- Drogue
- Site de streaming
- Réseaux sociaux

En plus de configurer les options souhaitées, toutes les modifications que vous apportez dans ce menu s'appliqueront au profil auquel vous avez associé l'application. Par conséquent, elles s'appliqueront également à tous les appareils que vous associez au profil. Pour plus d'informations sur la modification des profils, veuillez consulter la section « **Gérer les profils** » du portail Cyberfiltre Mobile.

Menu Contrôles :





Dans le menu Contrôles, vous disposerez des fonctionnalités « **Contrôle d'identité** » et « **Contrôle de site web** », analogues à la page présente dans le portail Cyberfiltre Mobile. Veuillez consulter la section « **Tableau de bord** » du portail de gestion pour plus d'informations sur ces fonctionnalités.

Pourquoi télécharger l'application Cyberfiltre Mobile Avancé ?

Nous vous recommandons de télécharger et d'installer l'application de protection WiFi & Antivirus « **Cyberfiltre Mobile Avancé** » afin d'être protégé sur n'importe quel appareil et notamment lorsque vous êtes connecté à un réseau WiFi.

Vous serez ainsi protégé que vous soyez connecté au réseau mobile Orange 4G/5G ou à n'importe quel réseau WiFi.

De plus, vous avez accès à l'option incluse dans l'application Antivirus, avec laquelle vous pouvez vérifier s'il y a des fichiers dangereux ou frauduleux sur votre appareil.