

## **Comment vérifier que le service « Sécurité Internet » de SFR Business est bien actif sur mon Réseau de ma Box Internet SFR ?**

Vous bénéficiez du service de protection « **Sécurité Internet** » qui vous protège de l'accès à de nombreuses ressources dangereuses de l'Internet comme des sites de diffusion ou de déclenchement de Malwares (comme les ransomware), de phishing ou encore des destinations illégales.

Et vous souhaiteriez vérifier si le service est bien actif sur vos postes ou votre réseau (LAN et Wifi).

Voici la procédure pour cela :

- 1. Positionnez-vous sur un ordinateur connecté au réseau de votre Box Internet SFR auquel vous pensez avoir le service d'activé.**

Nota : Le Service Sécurité Internet est proposé pour les accès Internet SFR Business de type :

- Box Business (sur ADSL ou Fibre Mutualisée)
- Connect Intégral (sur accès SDSL < ou = à 4 Mb/s)
- Connect Access et Connect Plus (sur ADSL ou Fibre Mutualisée)
- Access Max (sur ADSL)

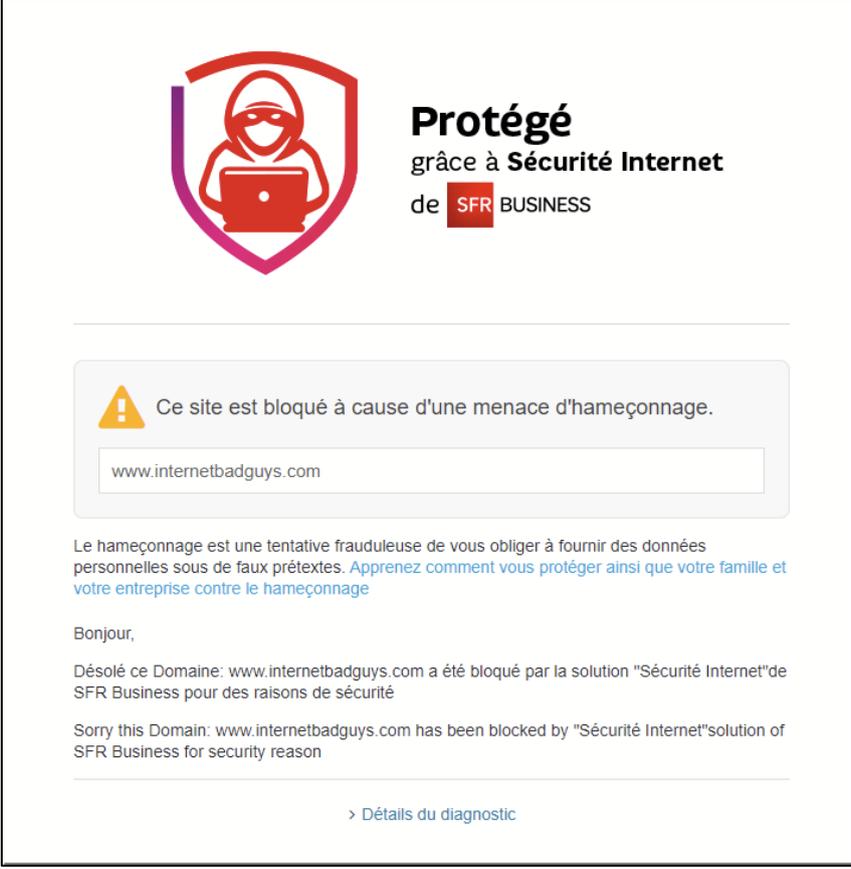
- 2. Ouvrir un navigateur (Chrome, Edge, Safari, Firefox, ...) sur ce poste**

Et taper l'URL suivante :

<http://www.internetbadguys.com> (site de test d'un site de phishing)

Si la page de blocage de la solution Sécurité Internet apparait dans votre navigateur, **vous avez la confirmation que le service est bien actif pour votre accès Internet SFR**

La page de blocage ressemble à ceci



**Protégé**  
grâce à **Sécurité Internet**  
de **SFR BUSINESS**

 Ce site est bloqué à cause d'une menace d'hameçonnage.

www.internetbadguys.com

Le hameçonnage est une tentative frauduleuse de vous obliger à fournir des données personnelles sous de faux prétextes. [Apprenez comment vous protéger ainsi que votre famille et votre entreprise contre le hameçonnage](#)

Bonjour,

Désolé ce Domaine: www.internetbadguys.com a été bloqué par la solution "Sécurité Internet"de SFR Business pour des raisons de sécurité

Sorry this Domain: www.internetbadguys.com has been blocked by "Sécurité Internet"solution of SFR Business for security reason

[> Détails du diagnostic](#)

Si au contraire une page de ce type apparait (ci-dessous), c'est que votre poste et, par déduction, le réseau sur lequel il est positionné n'est pas protégé par la solution.



**InternetBadGuys.com is only a demonstration site.**

If you were using OpenDNS,  
real phishing sites would be blocked.

**OpenDNS makes your Internet work better**

- **Safer:** helps prevent identity theft & blocks phishing sites.
- **Faster:** speeds up your existing Internet connection.
- **Smarter:** corrects spelling mistakes on the fly.

**Get started in 2 minutes**

It's **free** and there's no software to install. [Get started.](#)

**About this page**

David Ulevitch, the founder of OpenDNS, writes about Internet Bad Guys in "[Why I Started OpenDNS.](#)"

**OpenDNS**

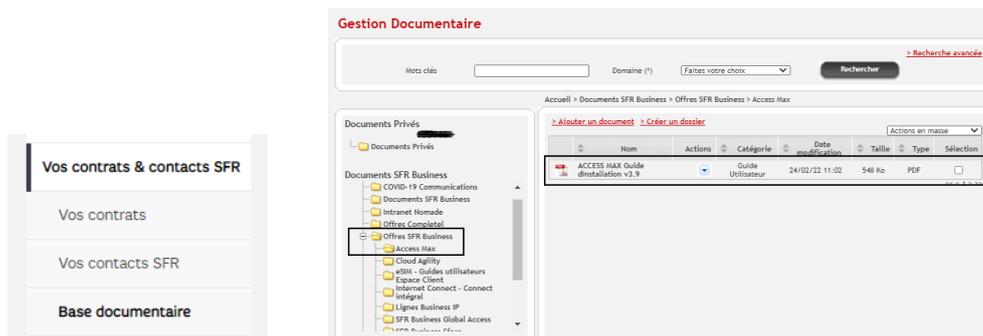
Plusieurs possibilités peuvent expliquer que le service n'est pas actif :

1. Le poste duquel vous faite le test **n'est pas connecté à la Box SFR Business** (vous êtes à votre domicile, connecté à votre mobile (partage de connexion), ou à un Wifi tiers), le service ne protège que le réseau (Lan et Wifi) directement connecté à la Box Internet SFR.
2. **Le Service n'est pas souscrit sur votre box** : reportez-vous à vos dernières factures ou [A VENIR] sur l'Espace Client SFR Business (<https://www.sfrbusiness.fr/espace-client/authentification/>) dans la rubrique « Votre Parc Fixe », Onglet « Gestion de vos Accès », retrouvez votre Accès Internet utilisé et en affichant le détail des options de votre offre de Box Internet SFR. Vous devez voir figurer l'option « Sécurité Internet ».
3. Vous avez peut-être **modifié volontairement la configuration DNS** sur votre poste ou sur votre réseau, ou sur votre serveur DHCP personnel : Pour que le service s'applique, il vous faut utiliser les DNS de SFR Business, qui sont diffusés et utilisés par défaut par votre Box Internet SFR Business.

Rappel : Les IP des DNS resolver SFR Business sont les suivantes :

Fournisseur DNS	Adresse Primaire	Adresse Secondaire
SFR Business	109.0.66.11	109.0.66.21

4. Vous avez configuré dans votre poste ou sur votre navigateur la fonction de « **DNS over Hhttps** » (DOH) qui fera que vous n'utiliserez plus les DNS de SFR Business.
5. Si vous êtes sur une accès Internet de type **Access Max sur raccordement ADSL**, vous devez avoir bien finalisé la configuration en mode « entreprise » de votre service. Reportez vous au guide d'installation de l'offre Access Max (disponible dans la base documentaire de l'Espace Client, dans le répertoire Access Max) [demande à connaître ses login/password PPP qui vous avait été transmis à la souscription de l'offre]



ou sur cette page spécialement créée <https://www.sfrbusiness.fr/assistance/solution-securite/finaliser-configuration-box-access-max-adsl-service-securite-internet.html>

APPENDIX :

Il existe d'autres pages de test de la solution pour simuler différents types de danger que la solution « **Sécurité Internet** » est capable de bloquer pour vous protéger.

- <http://www.internetbadguys.com> (site de test d'un site de phishing)
- <http://www.examplemalwaredomain.com> (site de test d'un site de malware, type Ransomware)
- <http://www.examplebotnetdomain.com> (site de test d'un site de contrôle d'un cybercriminel d'un réseau de Botnet)

Si le service est bien actif, il vous sera affiché la page de blocage de la solution.

- Fin