Hotspot et wifi partagé : précautions d'usage

Le réseau wifi partagé d'Orange est un réseau public qui vous permet d'accéder à internet. Vous devez observer quelques précautions d'usage pour utiliser les hotspots wifi d'Orange en toute sécurité.

Votre réseau wifi privé est sécurisé et vos échanges de données sont cryptés. Ce n'est pas le cas sur un réseau wifi public qui est ouvert à toute personne après une simple authentification.

réseau wifi privé

- Un réseau wifi privé est protégé par une clé de sécurité qui permet de crypter les échanges. Pour y accéder il est obligatoire de connaître cette clé de sécurité (clé WEP ou WPA/WPA2). L'équipement (ordinateur, tablette, mobile, console de jeux, ...) est autorisé à se connecter après avoir fourni cette clé de sécurité à la Livebox.
- Afin d'empêcher toute personne de pénétrer dans votre réseau privé sans fil, les connexions wifi sont chiffrées. Il est donc essentiel de sécuriser la connexion wifi de votre Livebox sans communiquer et sans désactiver votre clé de sécurité. À défaut, vous pouvez être tenu responsable des usages frauduleux qui auraient lieu via votre connexion internet.

réseau wifi public

Un réseau wifi public est en revanche accessible à tous par définition. Il n'y a pas de clé de sécurité pour protéger les échanges. Ce n'est pas l'équipement qui est autorisé à se connecter mais c'est l'utilisateur. L'utilisateur s'authentifie avec ses paramètres de connexion (identifiant et mot de passe).

L'absence de moyens cryptographiques sur les réseaux publics wifi introduit des possibilités de piratages par des individus malintentionnés :

- Écoute wifi, un pirate écoute les fréquences radio du wifi pour collecter des informations comme les identifiants et mots de passe qui ne sont pas protégés.
- Mise en place de faux hotspot (phishing), un pirate fabrique un faux hotspot wifi d'Orange et un faux portail d'authentification pour intercepter des informations sensibles.

Précautions d'usage :

Les risques de piratage sont diminués sur les sites sécurisés (préfixe https). Orange vous invite dans tous les cas à une vigilance accrue lors de vos accès à internet :

- Choisissez un mot de passe de messagerie Orange efficace. N'hésitez pas à le changer si vous pensez qu'un individu a pu vous le voler.
- Ne divulguez jamais vos identifiants de connexion.
- N'utilisez pas vos identifiants et mot de passe de messagerie sur d'autres sites qui pourraient les pirater et les réutiliser à votre insu. Vérifiez que la page d'accueil d'authentification Orange est bien la page habituelle.
- Lorsque vous vous connectez à un réseau wifi public, ne transmettez pas de données confidentielles comme par exemple vos coordonnées bancaires. Il peut y avoir un risque d'écoute des données transmises sur le réseau. Vos coordonnées et vos informations de carte bancaire ne seront jamais demandées sur la page d'accueil Orange.
- Assurez-vous que le site Web sur lequel vous vous connectez est sécurisé. Son adresse internet (URL) doit commencer par https:// et non par http://. Un cadenas fermé s'affiche dans votre navigateur internet (par exemple en bas à droite de la fenêtre ou à coté de l'adresse du site dans la

barre d'adresse). En double cliquant sur ce cadenas, une fenêtre s'affiche. Elle permet de visualiser les détails du certificat qui atteste que le site sur lequel vous êtes est bien le site sur lequel vous souhaitiez vous rendre.

- N'acceptez pas de certificat de sécurité d'origine inconnue, notamment au moment de la phase de connexion.
- Enregistrez vos identifiants de connexion lors des connexions sur le portail orange.fr. En cochant me reconnaître automatiquement lors de votre authentification, la connexion depuis la page d'accès wifi d'Orange est rapide et simple tout en diminuant les risques de piratage de vos identifiants.
- Si un message d'information vous indique que votre connexion est déjà utilisée, vérifiez si des personnes de votre foyer utilisent déjà l'accès wifi partagé.

Remarque : Lorsque vous êtes connecté à internet avec vos identifiants, si vous n'accédez pas normalement à internet, il est possible que vous soyez victime de phishing.le cas contraire il est souhaitable de modifier votre mot de passe en vous connectant à internet à votre domicile.

Identification : choisir votre mot de passe

Votre mot de passe Orange vous permet d'accéder à l'ensemble de vos services (Espace client, Mail, Cloud d'Orange...). Pour protéger cette accès ainsi que vos données personnelles, vous devez choisir un mot de passe personnalisé et sécurisé.
Lors de votre première identification sur orange.fr ou en cas de réinitialisation de votre mot de passe, vous devez choisir un mot de passe sécurisé qui protégera l'ensemble de vos données personnelles.
Ce mot de passe est strictement personnel et confidentiel. Assurez-vous de ne jamais le divulguer.

Pour assurer une parfaite confidentialité, votre mot de passe doit être sécurisé et difficile à trouver.

Mots de passe à éviter

Certains mots de passe trop évidents sont à proscrire : azerty, qwerty, abc123, password, 123456, 654321 ou 12345678 sont des exemples typiques de combinaisons n'offrant pas une sécurité suffisante.
Il est également recommandé d'éviter toute référence personnelle : date de naissance, prénom ou nom, société dans laquelle vous travaillez…
Ne choisissez pas votre mot de passe à partir d'un mot du dictionnaire.
Votre mot de passe ne doit pas reprendre, même partiellement, votre adresse mail. Ainsi, si votre adresse est cecile.bertau@orange.fr, des combinaisons telles que Cecile2014 ou bertau1930 ne sont pas adaptées.
Remarque : il est préférable d'utiliser un mot de passe différent pour chaque site ou usage différent. Ainsi, votre mot de passe Orange devrait être distinct de ceux que vous utilisez pour régler vos achats en ligne ou vous connecter aux réseaux sociaux par exemple.

Caractéristiques du mot de passe

Votre mot de passe doit comporter au minimum : 8 caractères. 1 majuscule. 1 minuscule. 1 chiffre.
Remarque : les symboles , . ; + : ! ? - _ sont autorisés.
Caractères non autorisés : Les lettres accentuées. Les espaces.

Votre mot de passe doit être mémorisable tout en étant suffisamment complexe pour ne pas être deviné. Quelques astuces existent pour concilier ces deux impératifs.

- La méthode phonétique

Cette technique consiste à choisir une phrase simple à retenir, et à utiliser les sons de chacune de ses syllabes comme caractères du mot de passe.
Ainsi, la phrase **J'ai acheté un DVD à 10 euros sur le cinéma** peut être transformée en mot de passe **ght1DVD10E@CN** par exemple.

- La méthode des premières lettres

Le mot de passe peut également être constitué des premières lettres des termes d'une phrase, complétées si besoin par de la ponctuation, des chiffres ou des majuscules :

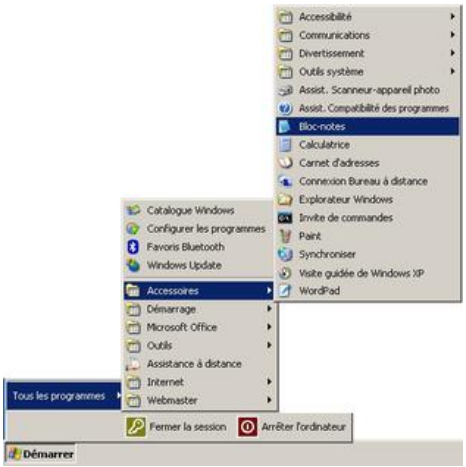
- Si vous décidez de créer votre mot de passe à partir du titre de la chanson **La complainte du phoque en Alaska**, la liste des premières lettres est **LcdpeA**.
- Il est préférable de ne pas utiliser la majuscule au début, le mot de passe devient donc **lcdpeA**.
- Le mot de passe n'est pas suffisamment sécurisé puisqu'il ne contient pas de chiffres ni de signes de ponctuation. La chanson a été composée en 1974, vous pouvez ainsi ajouter ce nombre à votre combinaison : **lc74:dpeA**.

Vous venez de créer un mot de passe complexe, que vous n'aurez aucune difficulté à retrouver.

Astuce pour saisir facilement la clé de sécurité

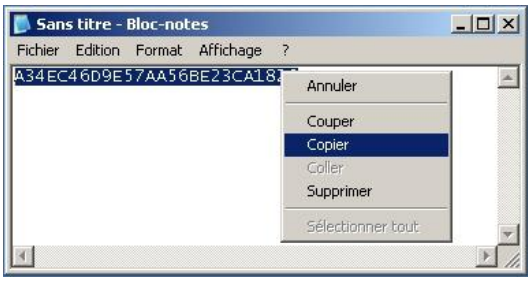
Il est quelquefois nécessaire de saisir la clé de sécurité de la Livebox, notamment lors d'une réinstallation ou d'une réinitialisation. Il faut toujours saisir deux fois la clé de sécurité : une première fois pour indiquer la clé, une deuxième fois pour confirmer la clé.
Voici comment saisir facilement la clé de sécurité de votre Livebox :

- *Lancez un logiciel éditeur de texte, par exemple le Bloc-notes de Windows. Pour lancer le Bloc-notes de Windows, cliquez sur les menus **Démarrer** > **Tous les programmes** > **Accessoires** > **Bloc-notes**.*



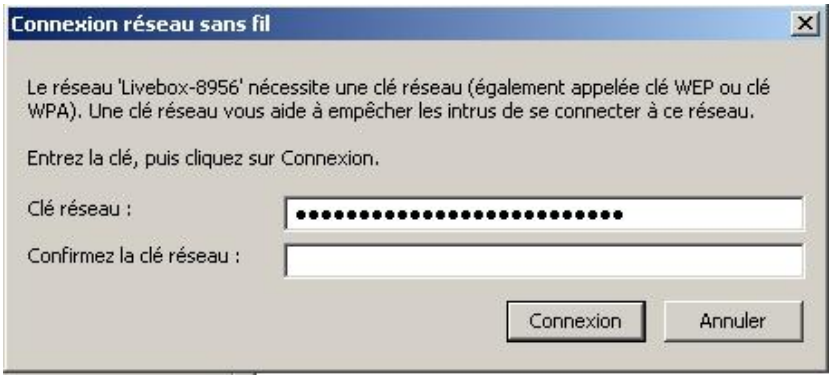
- *Dans la fenêtre qui s'ouvre, saisissez la clé de sécurité de votre Livebox.*

- *Une fois la clé saisie, sélectionnez-la puis copiez la. Pour cela, il suffit de presser simultanément les touches **CTRL + c** de votre clavier ou bien faites un clic droit avec la souris puis sélectionnez le menu **Copier**.*

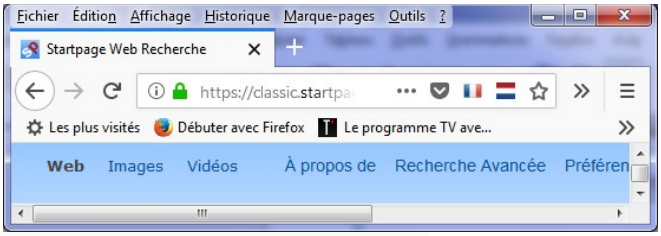


- *Collez la clé dans le champ de saisie de la clé de sécurité de la Livebox. Pour cela, il suffit de presser simultanément les touches **CTRL + v** de votre clavier ou bien faites un clic droit sur la souris puis sélectionnez le menu **Coller**.*

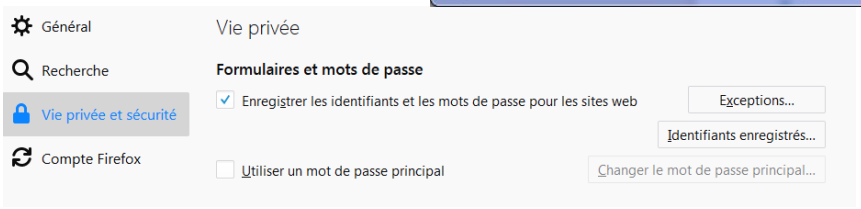
La clé de sécurité doit toujours être saisie deux fois. Recommencez l'opération dans le champ de confirmation.



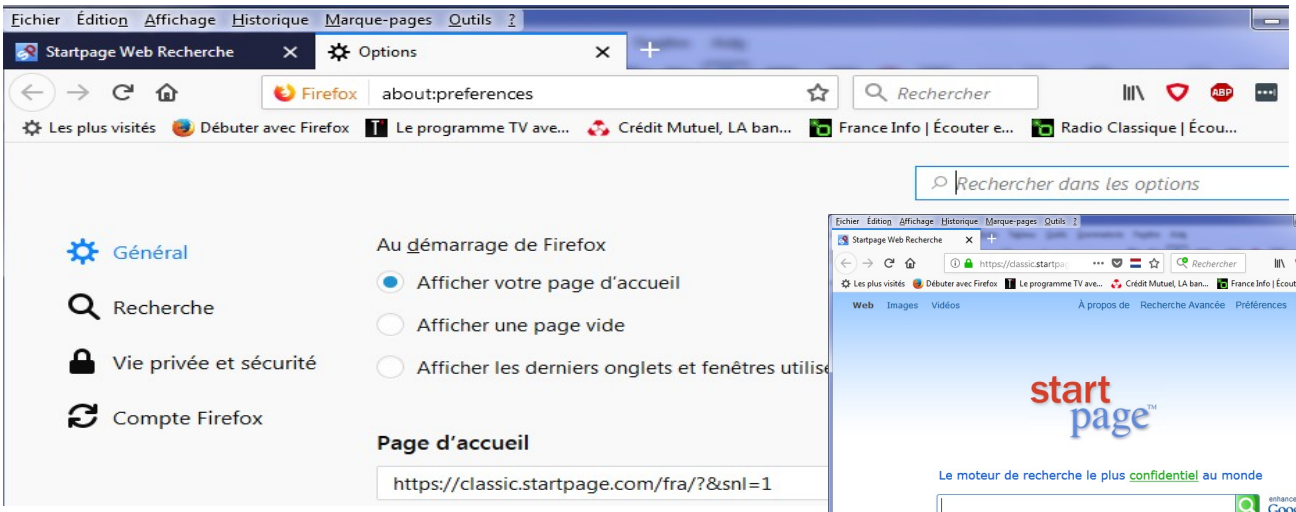
Précautions sur le navigateur (cas de Firefox de Mozilla) :



- Contrôler dans "Outils/Options/Vie privée et sécurité" si les **mots de passe** sont enregistrés, et dans l'affirmative, sécuriser avec un mot de passe principal !



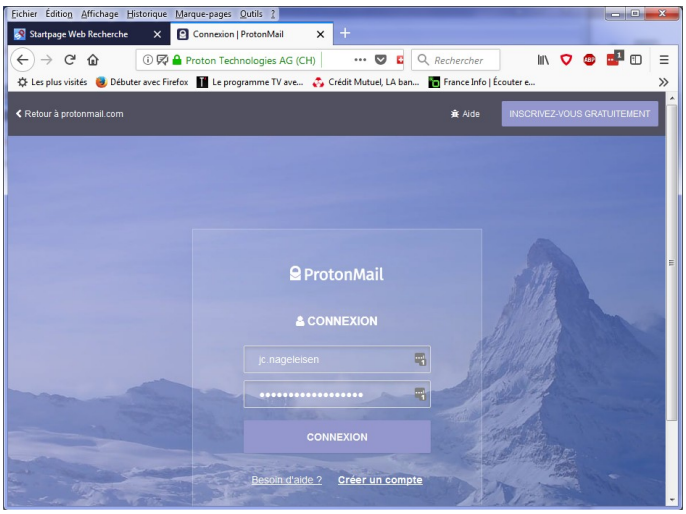
- Utiliser un "**moteur de recherche**" qui ne garde pas de traces de votre adresse IP ni de vos recherches (cookies de suivi) **ixquick** par exemple (www.ixquick.com) et son interface "startpage" et propose si besoin l'utilisation d'un "proxy" pour être totalement protégé.



- Utiliser un **"bloqueur" de publicité** (par ex **"Adbock plus"** pour limiter celles-ci...

ProtonMail, le plus grand service de messagerie chiffrée du monde

https://protonmail.com/fr/



ProtonMail est le premier service mondial de messagerie conçu afin de protéger la vie privée des utilisateurs. En utilisant le chiffrement de bout-en-bout, ProtonMail propose un plus grand respect la vie privée et plus de sécurité comparé aux autres entreprises de messagerie puisque la compagnie est incapable de lire les messages des utilisateurs. C'est la grande différence par rapport aux autres services de messagerie – comme par exemple Gmail – qui analysent activement les messages de leurs utilisateurs à des fins de marketing.