



Sécurité Wi-Fi : Protégez votre réseau domestique

Le Wi-Fi est devenu essentiel dans nos foyers. Sa sécurité doit être une priorité absolue.

Explorons ensemble comment protéger efficacement votre réseau sans fil.

j par julien catherine



Risques d'un Wi-Fi non protégé

Vol de données

Informations personnelles et bancaires interceptées par des pirates.

Utilisation parasitaire

Connexions non autorisées consommant votre bande passante.

Attaques malveillantes

Infiltration possible de virus et logiciels malveillants dans vos appareils.



Les protocoles de sécurité : WPA2 et WPA3

- 1 — WEP (Obsolète)
Protection faible, facilement contournable.
- 2 — WPA2
Sécurité standard. Chiffrement avancé AES.
- 3 — WPA3
Protection supérieure contre les attaques par force brute.

L'importance d'un mot de passe fort



12 caractères minimum

La longueur renforce considérablement la sécurité.



Caractères variés

Mélangez majuscules, minuscules, chiffres et symboles.



Phrase unique

Évitez dates de naissance et mots du dictionnaire.

Exercice guidé : Sécuriser son Wi-Fi (étape 1)



Accéder au routeur

Tapez 192.168.1.1 ou 192.168.0.1 dans votre navigateur.



Se connecter

Utilisez les identifiants admin (voir dessous du routeur).



Paramètres sans fil

Naviguez vers "Sécurité Wi-Fi" ou "Paramètres sans fil".



Sélectionner WPA2/WPA3

Choisissez le protocole le plus récent disponible.

Exercice guidé : Créer un mot de passe sécurisé (étape 2)



Vérifier la sécurité de son réseau

1

Analyser

Utilisez WiFi Analyzer pour scanner votre réseau.

2

Vérifier

Contrôlez la liste des appareils connectés régulièrement.

3

Tester

Essayez de vous connecter avec un mauvais mot de passe.



Conclusion et rappel des bonnes pratiques



Changez régulièrement

Modifiez votre mot de passe tous les trois mois.



Réseau invité

Créez un réseau séparé pour vos visiteurs.



Mises à jour

Actualisez le firmware de votre routeur régulièrement.



Discrétion

Ne partagez jamais votre mot de passe principal.

