culture
Saguenay–Lac-Saint-Jean

SÉCURISER VOTRE WI-FI & COMPRENDRE L'IMPORTANCE DES PARE-FEUX

Sécurisation complète de votre réseau Wi-Fi

Paramètres essentiels du routeur

- **Changer l'identifiant et le mot de passe administrateur**
  - Évitez les identifiants par défaut comme **admin/admin**.
- **Renommer le SSID (nom du réseau)**
  - Ne mentionnez ni votre nom, ni votre adresse ou fournisseur.

Créer un mot de passe fort pour le Wi-Fi

Au moins 12 caractères, incluant :

- ✓ Lettres majuscules et minuscules
- ✓ Chiffres
- ✓ Symboles

Exemple : **Réseau!Sécu#2024**

Mettre à jour le routeur régulièrement

- Téléchargez les **firmwares** depuis le site du fabricant.
- Activez les mises à jour automatiques si disponibles.

Chiffrement et protection d'accès

- **Utiliser le chiffrement WPA3**
  - WPA3 est le standard le plus sécurisé actuellement.
- **Désactiver le WPS (Wi-Fi Protected Setup)**
  - Cette fonction simplifie les connexions… et les intrusions !

Limiter les connexions et surveiller le trafic

- **Filtrage MAC** (adresse matérielle des appareils autorisés)
- **Vérifier régulièrement les appareils connectés**
- **Désactiver** le Wi-Fi quand vous ne l'utilisez pas (ex. : la nuit ou en vacances)

Créer un réseau invité

- **Séparer** le réseau principal des invités.
- **Restreindre l'accès** au réseau interne et aux fichiers partagés.

Autres conseils complémentaires

- **Désactivez l'accès à distance au routeur** si vous n'en avez pas besoin
- **Sécurisez physiquement votre routeur** (évitez les branchements publics)
- Utilisez un **DNS sécurisé** (ex. : Quad9, Cloudflare, OpenDNS)
- Surveillez les journaux d'accès de votre routeur
- Activez les notifications en cas de nouvel appareil connecté (selon modèle)

Un Wi-Fi sécurisé + un pare-feu actif = Moins de risques, plus de sérénité !

culture
Saguenay–Lac-Saint-Jean

Bonne pratique pour améliorer la couverture de votre réseau (WI-FI)

Bien placer votre routeur

- Placez-le au **centre de l'espace à couvrir**, à **hauteur moyenne** (pas par terre).
- Évitez de le **cacher** dans un meuble, une armoire ou derrière une TV.
- Éloignez-le des **sources d'interférences (micro-ondes, babyphones, objets métalliques).**

Éviter la saturation

- **Trop d'appareils** connectés peuvent **ralentir** le réseau.
- **Déconnectez** les appareils **inutilisés** ou configurez des **plages horaires d'accès**.

Utilisez un répéteur ou un système mesh

- **Répéteur Wi-Fi** : étend la couverture dans une autre pièce.
- **Système Wi-Fi mesh** : plusieurs bornes qui forment un seul réseau fluide (idéal pour grandes maisons ou bureaux).

Orientez correctement les antennes

- Si le routeur a des antennes, orientez-les à angles différents : une verticale et une horizontale pour couvrir plusieurs directions.

Connectez-vous à la bonne fréquence

- **2.4 GHz** : **portée plus large**, mais **plus lent** (idéale pour traverser les murs).
- **5 GHz** : **plus rapide**, mais **portée plus courte** (idéale à proximité).

Mettez à jour votre routeur

Vérifiez régulièrement les **mises à jour du firmware** pour bénéficier des dernières améliorations de performance et sécurité

Testez et ajustez

- Utilisez des applications comme **NetSpot**, **Wi-Fi Analyzer** ou **Speedtest** pour voir où le signal est faible.
- Déplacez le routeur ou ajoutez un répéteur en fonction des résultats.

culture
Saguenay–Lac-Saint-Jean

L’importance des PARE-FEUX (Firewalls)

Un pare-feu agit comme un filtre entre votre appareil et Internet, bloquant les accès non autorisés.

Pourquoi activer un pare-feu ?

- **Filtrage du trafic réseau**
  - analyser les données entrant et sortant d’un ordinateur ou d’un réseau
  - bloquer le trafic non autorisé et autoriser que ce qui correspond aux règles établies
- **Protection contre les attaques externes**
  - empêcher les pirates d’accéder directement à un système
  - bloquer certaines attaques comme les scans de ports, les tentatives d’intrusion, etc..
- **Contrôle des applications et des utilisateurs**
  - gérer quels programmes ou utilisateurs ont accès à Internet
  - limiter la fuite de données et empêcher les applications malveillantes de communiquer sans autorisation
- **Surveillance et journalisation**
  - garder une trace du trafic réseau (logs).
  - détecter des comportements suspects utile pour enquêter en cas d’incident.
- **Sécurité dans les réseaux d’entreprise**
  - Dans une organisation, un pare-feu protège les serveurs, postes de travail et données sensibles.
  - Permet de séparer aussi différents segments du réseau (par exemple, réseau interne vs. accès invité).

Bonnes pratiques liées aux pare-feux

- **Toujours** laisser le pare-feu **activé**, même à la maison
- **Configurer** des règles personnalisées pour bloquer ou autoriser certains services
- **Ne pas désactiver** le pare-feu même si un logiciel vous le propose
- Vérifiez régulièrement les alertes ou tentatives bloquées

Types de pare-feux

Type	Description
Pare-feu matériel	Souvent intégré au modem ou routeur, ou relié à ces derniers
Pare-feu logiciel	Intégré dans les systèmes d’exploitation Windows/Unix ou applications tierces
Pare-feu d’entreprise	Solutions avancées (IA, filtrage, inspection, journalisation)