Comment protéger votre réseau

Article qui focus sur les réseaux domestiques

Est-ce que l'accès à internet et la protection de votre vie privée vous préoccupe?

Article numéro un

Focus sur HELIX de Vidéotron

Comment protéger l’accès à Internet et la vie privée sur votre réseau domestique

Comment protéger l’accès à Internet et la vie privée sur votre réseau domestique

Biais au sujet des services et produits HELIX de Vidéotron

Si vous voulez protéger votre **accès à Internet**, votre **vie privée** et tous les **appareils** de votre réseau domestique (routeur, modem/routeur combiné, téléphones, ordinateurs, etc.), voici des astuces et conseils pratiques.

Mesures essentielles

1. **Changer le mot de passe administrateur par défaut**
   - Définissez un mot de passe unique et long pour l’administrateur du routeur

     ≥16 caractères, mélange de lettres, chiffres et symboles

     Explication
     Le mot de passe par défaut est souvent connu ou imprimé sur le routeur. Si quelqu’un le connaît, il peut accéder à votre réseau et le modifier.
2. **Mettre à jour le firmware**
   - Vérifiez le logiciel interne de votre routeur/modem (firmware) et appliquez toutes les mises à jour fournies par le fabricant.

     Explication
     Le firmware est le logiciel intégré au routeur. Les mises à jour corrigent des failles de sécurité et améliorent la stabilité.
3. **Utiliser un chiffrement Wi-Fi fort**
   - Assurez-vous d’utiliser le protocole **WPA3**, ou au minimum **WPA2-AES**.

     Explication
     Le chiffrement protège les données transmises sur votre réseau Wi-Fi. WPA3 est le plus récent et le plus sûr.

4. **Choisir un SSID non identifiable**
   - Nommez votre Wi-Fi avec un nom neutre (évitez votre nom ou adresse). Il n'est pas nécessaire de le cacher (SSID visible).

> Explication
> Le SSID est le nom du réseau Wi-Fi. Le cacher n'apporte pas de vraie sécurité, mais le chiffrement et le mot de passe le font.

5. **Définir un mot de passe Wi-Fi fort**
   - Utilisez une longue phrase de passe Définissez un mot de passe unique et long pour l'administrateur du routeur

     ≥16 caractères, mélange de lettres, chiffres et symboles

     . Un gestionnaire de mots de passe peut vous aider.

> Explication
> Un mot de passe complexe empêche les intrusions par devinettes ou attaques automatisées.

6. **Activer le pare-feu du routeur**
   - Assurez-vous que le pare-feu intégré est activé et bloque les connexions non sollicitées. Le NAT par défaut + pare-feu est suffisant pour une utilisation domestique.

> Explication
> Le pare-feu protège votre réseau contre les accès extérieurs. Le *NAT* (Network Address Translation) permet de partager une seule IP publique entre plusieurs appareils tout en limitant les accès entrants.

Changements de configuration importants

1. **Désactiver la gestion à distance**
   - Empêche d'accéder à l'interface du routeur depuis Internet.
   - Si nécessaire, utilisez un **VPN** avec authentification forte.
2. **Désactiver WPS (Wi-Fi Protected Setup)**
   - WPS peut être exploité par des attaquants pour accéder au réseau.
3. **Désactiver UPnP sur le WAN**
   - UPnP (Universal Plug and Play) permet aux applications de créer automatiquement des règles de pare-feu, mais peut ouvrir des failles de sécurité.
4. **Désactiver les services inutiles**
   - Exemple : Telnet, protocoles anciens ou fonctionnalités cloud inutilisées.
5. **Créer un réseau invité**
   - Pour les visiteurs et les appareils non fiables.
   - Isolé du réseau principal, avec mot de passe séparé et, si possible, VLAN différent.
6. **Segmenter les appareils IoT**
   - Les appareils connectés (caméras, TV intelligentes, capteurs) sont souvent vulnérables. Les

mettre sur un réseau séparé réduit les risques.

7. **Utiliser des réservations DHCP / IP statiques**
   - Facilite le suivi des appareils et l'application de règles de sécurité.

Confidentialité et chiffrement

1. **DNS-over-HTTPS (DoH) ou DNS-over-TLS**
   - Empêche l'espionnage des requêtes DNS locales.
   - Exemples : Cloudflare (`1.1.1.1`), Quad9 (`9.9.9.9`).
2. **VPN**
   - *Par appareil :* protège la vie privée sur mobile ou PC.
   - *Au niveau du routeur :* chiffre tout le trafic du réseau, mais peut réduire la vitesse et gêner certains services géolocalisés.
3. **HTTPS Everywhere**
   - Toujours utiliser des sites sécurisés (TLS/HTTPS).
4. **Authentification à deux facteurs (2FA)**
   - Ajoute une couche de sécurité sur vos comptes importants (email, cloud, routeur).

Mesures avancées pour utilisateurs expérimentés

1. **Installer un firmware alternatif**
   - OpenWrt, DD-WRT ou Tomato peuvent offrir pare-feu avancé, VLAN, QoS et plus.
   - ⚠ Ne le faites que si vous savez ce que vous faites : un mauvais flash peut endommager le routeur.
2. **Utiliser un OS routeur/firewall dédié**
   - pfSense ou OPNsense permettent pare-feu professionnel, IDS/IPS, VPN, VLANs, contrôle précis.
3. **IDS/IPS (Intrusion Detection/Prevention)**
   - Surveille et bloque le trafic suspect. Exemples : Suricata, Snort.
4. **Configurer des VLANs**
   - Séparer admin, IoT, invités.
   - Les VLAN empêchent certains appareils d'accéder à d'autres réseaux internes.
5. **Bloquer les ports et limiter le port forwarding**
   - N'ouvrez que les ports nécessaires et restreignez-les à des IP internes fiables.

Pour un modem/routeur combiné

- Si vous avez un routeur séparé fiable, mettez le modem en **mode bridge** pour que le routeur gère NAT et pare-feu.
- Si vous devez utiliser l'appareil de l'ISP, désactivez le Wi-Fi et utilisez votre propre routeur pour le Wi-Fi.

Surveillance et maintenance

1. **Journalisation et surveillance**
   - Activez les logs et vérifiez régulièrement les connexions inhabituelles.
2. **Scan réseau**
   - Utilisez Fing ou Nmap pour identifier les appareils connectés.
3. **Rotation des mots de passe et vérification des appareils**
   - Supprimez les appareils inconnus et les comptes obsolètes.
4. **Sauvegarde de configuration**
   - Exportez les réglages sécurisés pour restaurer facilement le routeur.

Hygiène comportementale et des appareils

- Maintenir les appareils à jour.
- Utiliser antivirus si nécessaire.
- Éviter les liens dans les emails suspects (phishing).
- Limiter les droits administrateur sur les ordinateurs quotidiens.

Paramètres concrets pour l'interface Helix

- **Accès admin :** HTTPS seulement, local uniquement (désactiver WAN).
- **Wi-Fi :** SSID = `HomeNetwork`, sécurité WPA3 ou WPA2-AES, mot de passe long Définissez un mot de passe unique et long pour l'administrateur du routeur

  ≥16 caractères, mélange de lettres, chiffres et symboles
- **Wi-Fi invité :** isolation activée, mot de passe séparé.
- **UPnP :** OFF
- **WPS :** OFF
- **Gestion à distance :** OFF
- **Pare-feu :** refuser tout inbound, autoriser le trafic établi.
- **DHCP :** réserver les IP pour téléphones/PC, baux plus courts pour invités/IoT.