FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

CONNAISSEZ-VOUS VOTRE ROUTEUR ?

ROBERT ARSENEAULT

18 JANVIER, 2024

TABLE DES MATIÈRES

1. APRÈS INSTALLATION, EST SOUVENT OUBLIÉ

- Routeur est **lien** entre l'Internet et appareils incluant le Wi-Fi;

- **Vie typique** d'un routeur est de 5 à 10 ans. Remplacé pour la compatibilité avec normes Wi-Fi récentes (vitesse et sécurité), connections avec appareils additionnels, corriger problèmes de connectivités ou suivant l'arrêt des mise-à-jours. Notons le remplacement par votre Fournisseur de service peut aussi avoir certains avantages, et présentement convertir vers la technologie **Wi-Fi 6E** (802.11ax-2021) peut valoir la peine.

- Routeurs sur le marché **ne présentent pas tous les mêmes caractéristiques et les mêmes performances**. Beaucoup de termes techniques utilisés, peuvent être source fréquente de confusions chez les moins techno. Ceci peut compromettre l'étanchéité de la sécurité et intéresser des pirates;

- Étude du <National Institute of Standards and Technology> en 2022 (grande période de télétravail), avait **identifié plus de 209 failles de sécurité** parmi les marques de routeurs.

2. REVUE EXIGENCES: SÉLECTION ROUTEUR

- Les constructeurs rivalisent en technologie pour développer des modèles toujours plus performants afin de répondre aux besoins de plus en plus exigeants des utilisateurs. En exemple, nouveau routeur va probablement supporter le **WPA3**, la norme la plus récente de sécurité;

- Certains modèles très basiques utilisé uniquement dans un cadre domestique par *un très petit groupe de personnes alors que d'autres peuvent répondre aux besoins professionnels* qui exploitent plusieurs dizaines d'appareils connectés en même temps.

- L'achat d'un routeur est question de budget et de choix en fonction des besoins. Modèle basique suffira si on compte utiliser l'appareil en milieu domestique par un petit groupe de personnes. Si vous avez besoin d'une connexion de très haut débit pour certaines opérations (lecture de vidéo HD ou jeux en ligne) domestiques ou professionnelles, un routeur plus puissant et donc plus cher sera requis.

3. CRITÈRES LORS DE LA REVUE OU ACHAT

- **Le débit** : majorité des routeurs Wifi proposent des débits satisfaisants en mode filaire. Le débit sans fil est donc le plus important. Certains modèles présentent parfois *une grande perte de débit en Wifi*. Le taux de transfert est ainsi réduit.

- **La stabilité** : étroitement liée au débit, la stabilité de transfert dépend également de la puissance du routeur. Préférez modèles puissants si vous comptez effectuer plusieurs tâches lourdes en même temps pour *profiter d'une vitesse de transfert stable*.

- **La portée** : zone dans laquelle votre réseau sera accessible. Les obstacles comme les murs peuvent réduire cette portée. N'oublions pas que le trajet entre le routeur et votre équipement peut aussi être influencé par les présence des matériaux de métal, interférences Bluetooth, micro-ondes, etc. La portée devra donc être *considérée en même temps, que la configuration de votre logement*.

3. CRITÈRES LORS DE LA REVUE OU ACHAT

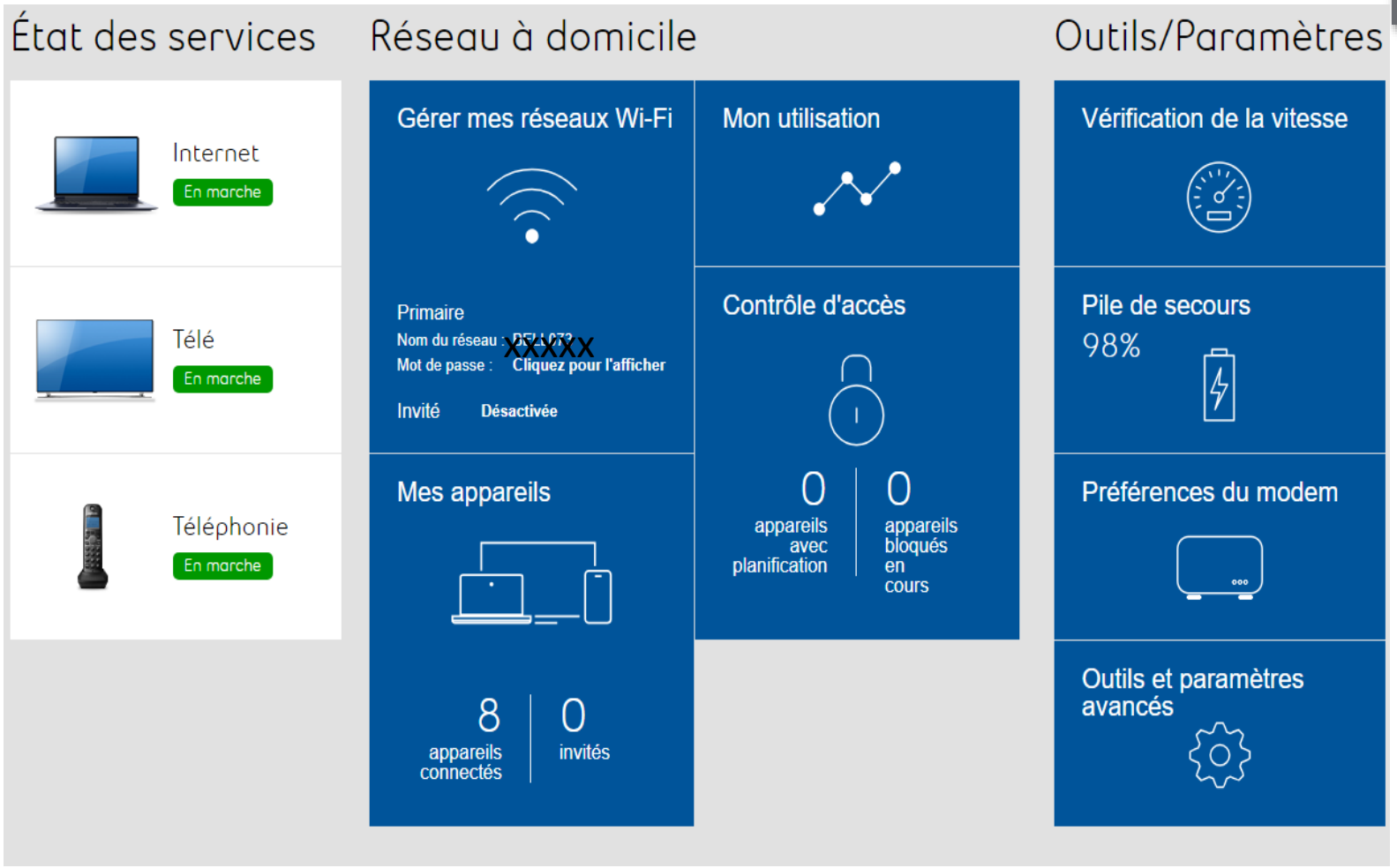
- **La sécurisation** : en plus du contrôle parental, un bon routeur doit être capable de sécuriser le réseau par un *contrôle de chaque adresse IP connecté*. Routeurs proposent aujourd'hui des systèmes de chiffrement efficaces (clés WPA…) pour mieux protéger votre réseau et mieux contrôler les accès.

- **La facilité d'installation** : critère très important si vous disposez de connaissances limitées dans le domaine. En principe, *la venue d'un installateur ne sera pas requise* si le modèle est facile à installer. Choisissez également les modèles faciles à configurer (assistance et firmware de configuration fournis…).

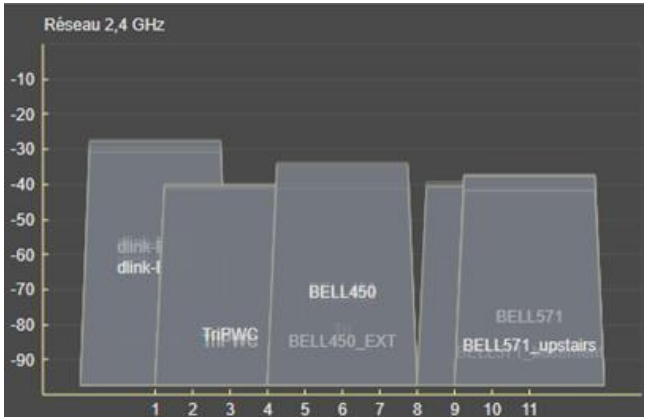
- **Le prix** : les prix des routeurs *dépendent des caractéristiques techniques du modèle*. L'achat d'un modèle haute performance est facilement un multiple du prix d'un modèle basique.

4. ÉLÉMENTS TYPIQUES DE ROUTEUR

- Un exemple parmi d'autres :



4. ÉLÉMENTS TYPIQUES DE ROUTEUR



Paramètres du modem et outils diagnostics pour utilisateurs plus avancés.

Réseau

- DMZ >
- DDNS (DNS dynamique) >
- DHCP >
- Redirection de port >
- UPnP I O
- DLNA I O
- SIP ALG I O

Wi-Fi

- WPS >
- Filtrage MAC >
- Analyseur de réseau Wi-Fi >

Modem

- À propos >
- DNS >
- WAN >
- Sauvegarde / Restaurer
  - Sauvegarde
  - Restaurer

Outils

- Statistiques >
- Journaux système >
- Utilitaires >
- Surveillance >
- Ethernet >
- Réinitialisation >
- Diagnostics >

5. ÉVOLUTION DES GÉNÉRATIONS DE WI-FI

Générations Wi-Fi				
Génération	Norme IEEE	Date Adopté	Debit lien Maximum (Mbit/s)	Fréquence Radio (GHz)
Wi-Fi 7	802.11be	(2024)	1376–46120	2.4, 5, 6
Wi-Fi 6E	802.11ax	2020	574–9608[1]	6[a]
Wi-Fi 6		2019		2.4, 5
Wi-Fi 5	802.11ac	2014	433–6933	5[b]
Wi-Fi 4	802.11n	2008	72–600	2.4, 5
(Wi-Fi 3)*	802.11g	2003	6–54	2.4
(Wi-Fi 2)*	802.11a	1999		5
(Wi-Fi 1)*	802.11b	1999	1–11	2.4
(Wi-Fi 0)*	802.11	1997	1–2	2.4

***Wi-Fi 0, 1, 2, and 3 are named by retroactive inference.**
They do not exist in the official nomenclature.

Source: Wikipedia IEEE 802.11be

5. ÉVOLUTION DES GÉNÉRATIONS DE WI-FI

- Mais comment savez-vous quelle norme Wi-Fi choisir ? Eh bien, cela dépend si les appareils que vous possédez prennent en charge le **Wi-Fi 6** ou non. Quand le Wi-Fi 6 est devenu la norme en 2019, la plupart des fabricants ont commencé à créer des appareils qui prennent en charge la norme. Cependant, les routeurs Wi-Fi 6 sont également rétro-compatibles**.** Ainsi, vous investissez dans un routeur à l'épreuve du temps capable de prendre en charge les appareils compatibles Wi-Fi 6. Le Wi-Fi 6 utilise moins d'énergie que le Wi-Fi 5, offre une meilleure sécurité, des vitesses plus élevées et est généralement plus fiable dans des environnements plus occupés.

- La capacité de l'unique bande initiale des fréquences du **réseau 2,4 GHz** , augmentait très rapidement, nécessitant la création d'une deuxième bande de fréquences dans **le 5,0 GHz.** *Notons aussi que plus la fréquence est élevée, plus la vitesse de transmission augmente.* Avec la continuation des besoins, une **nouvelle bande de 6,0 GHz** est maintenant disponible depuis peu. Ce qui a exigé beaucoup de coordination avec les entités de réglementations gouvernementales des pays.

5. ÉVOLUTION DES GÉNÉRATIONS DE WI-FI

- La nouvelle norme **Wi-Fi 7** promet des améliorations dans tous les aspects du Wi-Fi, y compris le débit, la qualité de la connexion et la portée. Enfin, nous pourrions avoir une connexion Wi-Fi qui peut maintenir de véritables vitesses multi-Gigabits**,** assez rapide pour fournir 10Gbps Internet. Cependant, il est important de garder ce qui suit à l'esprit :

- Les améliorations du Wi-Fi 7 ne s'appliquent qu'aux clients pris en charge - ceux avec la bande de 6 GHz, avec entre autres **EHT** (**E**xtremely **H**igh **T**hroughtput wireless, entre 30 et 40 Gbps);

- Les clients déjà existants, y compris certains Wi-Fi 5 et tous les Wi-Fi 4 et anciens, ne seront plus entièrement pris en charge par les diffuseurs Wi-Fi 7 en raison des exigences de sécurité plus élevées (WPA2 ou WP3). (La bande de 6 GHz nécessite toujours WPA3). Certains routeurs avec Wi-Fi 7 ont commencé à être offert, après la ratification Wi-Fi **début 2024.**

6. SÉCURITÉ DU WI-FI

- Wired Equivalent Privacy (**WEP**) date de 1997. N'est plus assez sécuritaire, car il existe des logicies pour le <craquer>);

- Wi-Fi Protected Access (**WPA**) daté de 2004;

- Wi-Fi Protected Access II (**WPA2**). WPA2 emploie un chiffrement par bloc appelé **Advanced Encryption Standard (AES)** pour former la base de son protocole de cryptage. Selon votre routeur, **choisir WPA2 peut ne pas être assez bon.**

- Wi-Fi Protected Access III (**WPA3**) date de 2018. Contrairement à ses prédécesseurs, WPA3 offre également la confidentialité persistante (voir explication Wikipedia). Cela ajoute l'avantage considérable de protéger les informations précédemment échangées, même si une clé secrète à long terme est compromise. Les routeurs plus anciens n'ont pas **WPA3,** et les appareils plus anciens ne peuvent pas utiliser WPA3. Mais si vous avez un nouveau routeur qui prend en charge WPA3 et tous les appareils plus récents, vous devriez passer à WPA3.

6. SÉCURITÉ DU WI-FI

- WPA2 et WPA3 restent vos meilleurs choix pour la sécurité Wi-Fi. La désapprobation de WEP et WPA est assez récente, il est possible dans grandes organisations ainsi qu'a la maison de trouver du matériel plus ancien qui utilise toujours ces protocoles. Si vous ne pouvez pas **utiliser WPA2 ou WPA3**, faites de votre mieux pour prendre des mesures de sécurité supplémentaires. Le meilleur rapport qualité-prix est d'utiliser un réseau privé virtuel (VPN). L'utilisation d'un **VPN** est une bonne idée, quel que soit le type de cryptage Wi-Fi que vous avez. Sur le Wi-Fi ouvert (cafés) et utilisant WEP, il est tout simplement irresponsable de se passer d'un VPN. C'est comme crier vos coordonnées bancaires en commandant votre deuxième cappuccino.

- Le protocole TKIP (Temporal Key Integrity Protocol) et l'Advanced Encryption Standard (AES) sont deux types de chiffrement différents qui peuvent être utilisés par un réseau Wi-Fi. Alors que WPA2 est censé utiliser AES pour une sécurité optimale, il peut également utiliser TKIP, où la rétro-compatibilité avec les périphériques hérités est nécessaire. **TKIP n'est plus considéré comme sécurisé et est maintenant obsolète.** Vous ne devriez pas l'utiliser. WPA2, développé en 2004 par la Wi-Fi Alliance, est la **norme de sécurité minimale absolue** que vous devriez rechercher dans un routeur. En cas de doute, **choisissez toujours WPA 2 (AES) ou WPA3.**

6. SÉCURITÉ DU WI-FI

- Pour utiliser WPA3, votre ordinateur portable, smartphone et autres appareils doivent également être compatibles avec le protocole de sécurité.

- Selon Microsoft, Windows 11 et Windows 10 (version 2004) prennent tous deux en charge le Wi-Fi 6 et WPA3. De nombreux appareils d'Apple prennent également en charge le protocole, à commencer par l'iPhone 7, l'iPad de 5e génération, l'Apple Watch Series 3, l'Apple TV 4K et ses ordinateurs Mac fin 2013. Android 10 a introduit la prise en charge de WPA3 en 2019.

- Pour les appareils domestiques intelligents qui se connectent à votre réseau, vérifiez auprès du fabricant si un équipement individuel prend en charge le protocole de sécurité. L'Alliance Wi-Fi continuera également de prendre en charge WPA2 dans un avenir prévisible.

7.INTÉRÊTS DES PIRATES POUR Y AVOIR ACCÈS

- Pirater un routeur, c'est un peu comme pirater votre ordinateur. Les criminels ciblent généralement les mots de passe ou les paramètres de sécurité faibles. Accèdent au routeur, ils utilisent du code malveillant (malware) pour accéder à votre réseau.

- Ayant piraté votre routeur, il est facile pour eux d'accéder à tout ce qui y est connecté. Cela comprend les caméras de sécurité, les ordinateurs, les téléviseurs intelligents et même les appareils électroménagers. Ainsi ils peuvent regarder à travers vos caméras, accéder à des comptes bancaires et plus encore.

- Ils peuvent également utiliser votre connexion Internet pour faire des choses néfastes, illégales comme envoyer des e-mails de phishing ou pirater la technologie ou les comptes d'autres personnes. Suivi de leur activité est plus difficile a retracé, car c'est votre réseau avec votre nom qui paraitra et pas eux.

7.INTÉRÊTS DES PIRATES POUR Y AVOIR ACCÈS

- « Le contrôle du routeur permet aux utilisateurs malveillants de surveiller, capturer et manipuler les données envoyées et reçues », « Ils peuvent rediriger les utilisateurs vers des sites Web malveillants ou propager des logiciels malveillants à d'autres appareils. Les attaquants peuvent également exploiter les routeurs compromis pour attaquer d'autres systèmes et masquer leur véritable adresse IP à l'aide du réseau de la victime.

- Exemple de malware de routeur VPNFilter est l'un des types les plus populaires de logiciels malveillants de routeur, responsable de plus d'un demi-million d'attaques. Il s'étend à toute technologie connectée aux routeurs, recueillant des informations personnelles telles que les mots de passe de compte, les informations bancaires et les numéros de sécurité sociale.

8. COMMENT CONFIRMER SI PIRATAGE

Il y a plusieurs indices à rechercher :

- **Vitesse lente de l'ordinateur ou d'Internet** : Les logiciels malveillants peuvent réduire les performances de votre technologie. C'est l'un des signes les plus sûrs que votre réseau peut être compromis.

- **Vos mots de passe ne fonctionnent pas** : si cela se produit tout d'un coup, cela peut signifier que les pirates les ont changés.

- **Redirections de sites Web** : Les escrocs peuvent rediriger votre navigateur vers des sites faux ou malveillants qui peuvent infecter votre système avec encore plus de logiciels malveillants. Ces sites peuvent également vous inciter à entrer des informations personnelles, telles que votre numéro de sécurité sociale ou de compte bancaire.

8. COMMENT CONFIRMER SI PIRATAGE

- **Fausses notifications antivirus** : Celle-ci est délicate. En vous faisant croire que vous êtes infecté, ils vous infectent. L'objectif : amener à télécharger la protection contre le virus supposé. Au lieu de cela, vous téléchargez vraiment des logiciels malveillants. Ou ils peuvent vous tromper en achetant de faux logiciels antivirus.

- **Nouvelles applications ou logiciels** : Si vous remarquez nouvelles applications ou de nouveaux logiciels sur votre ordinateur, tablette ou téléphone et que vous êtes sûr de ne pas l'avoir téléchargés, votre réseau peut être compromis. Les pirates informatiques ont peut-être installé ces éléments pour infiltrer votre technologie.

- **Appareils inconnus** : Si vous vous connectez à l'interface administrateur de votre routeur et que vous voyez des appareils connectés que vous ne reconnaissez pas, vous avez probablement été piraté. Explorez noms des fournisseurs d'équipements, en utilisant l'adresse MAC vérifiant avec https://macvendors.com/. Ou l'application <Wireless Network Watcher> pour liste des présences.

9. COMMENT PRÉVENIR LE PIRATAGE

- Bien que se faire pirater puisse sembler effrayant, il existe plusieurs façons de vous protéger et de protéger votre routeur.
- Il s'agit notamment de changer vos mots de passe (suggère 14 charactères minimum ou les passkeys), de mettre à jour votre routeur et d'ajouter des mesures de sécurité.
- Modifiez également votre mot de passe Wi-Fi pendant que vous y êtes. Si vous ne savez pas comment changer les mots de passe, faites une recherche en ligne avec le nom de votre routeur et « comment changer le mot de passe administrateur » pour obtenir des instructions.
- Le firmware obsolète du routeur est un autre problème courant, selon Amishave. Les micrologiciels vulnérables peuvent être exploités pour obtenir un accès non autorisé. Assurez-vous de mettre à jour votre routeur une fois par mois.

10. LIMITER LA VULNÉRABILITÉ AU PIRATAGE

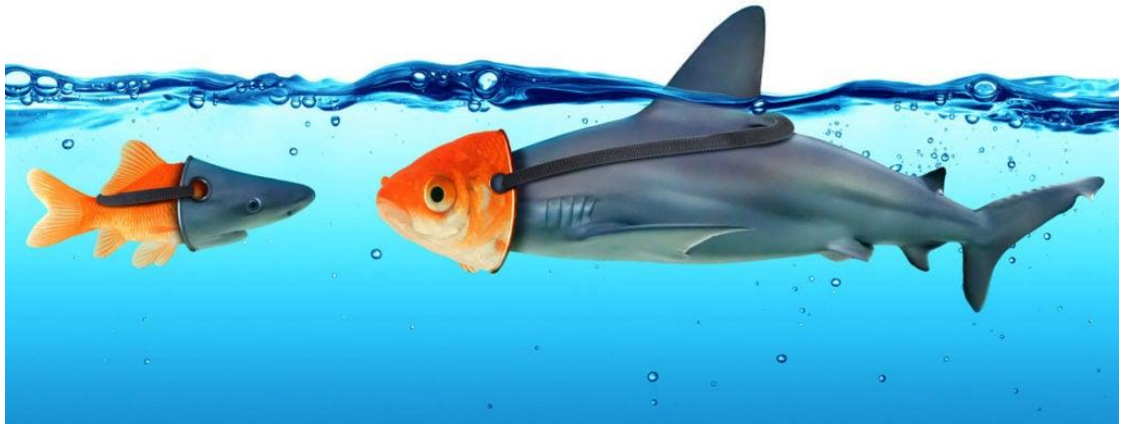
Voici d'autres étapes pour rendre votre réseau moins vulnérable au piratage :

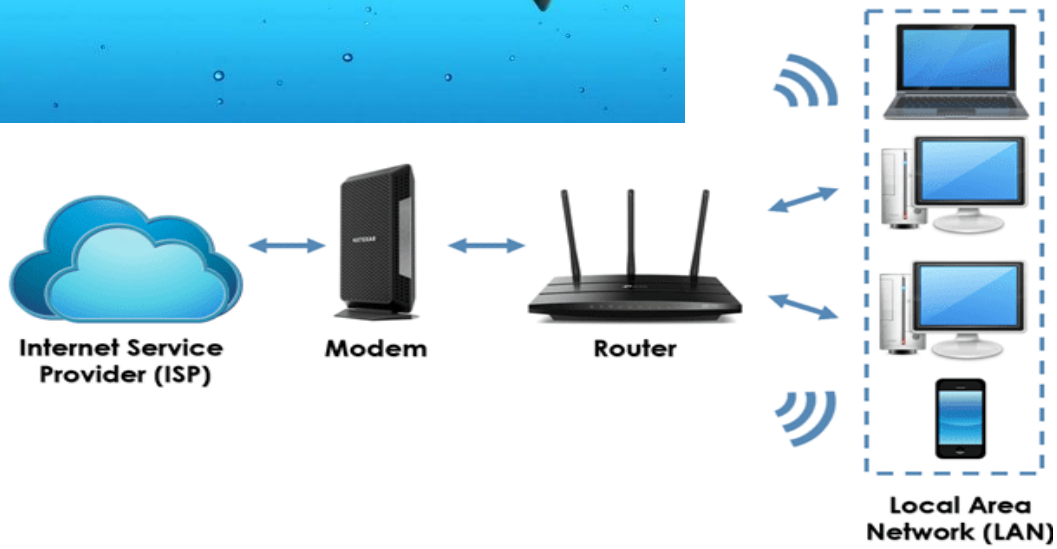
- Veillez à désactiver toute fonctionnalité de gestion à distance.
- Utilisez le cryptage WPA3 ou WPA2 pour votre Wi-Fi. Si votre routeur est plus ancien, il peut seulement utiliser le cryptage WPA et WEP. Dans ce cas, mettez à niveau vers un nouveau routeur avec le cryptage WPA3 ou WPA2.
- Désactivez les options Wi-Fi Protected Setup (WPS) et Universal Plug and Play (UPnP) dans les paramètres de votre routeur. Cela rendra plus difficile pour les pirates d'y accéder.
- Envisagez de configurer un réseau invité pour les visiteurs ou les appareils non fiables. Cela empêchera les autres d'avoir votre mot de passe principal, protégeant ainsi votre réseau contre les logiciels malveillants qui peuvent se trouver sur les ordinateurs ou les téléphones de vos amis.

10. LIMITER LA VULNÉRABILITÉ AU PIRATAGE

- Assurez-vous que le pare-feu intégré du routeur est activé.

- Envisagez d'utiliser **un VPN sur votre routeur** pour une confidentialité et une sécurité accrues.





11. QUOI FAIRE SI PIRATÉ

Si vous pensez avoir été piraté, prenez les mesures suivantes :

- Connectez-vous à l'interface administrateur de votre routeur et déconnectez tous les appareils inconnus de votre réseau. Réinitialisez ensuite les paramètres d'usine de votre routeur. (Au préalable il aurait fallu enregistrer la configuration que vous ou le technicien y a installé)

- Remplacez le mot de passe par de votre routeur. Assurez-vous que c'est un mot de passe fort avec des chiffres, des lettres et des symboles.

- Analysez votre système avec un logiciel antivirus pour détecter tout code malveillant. Ne pensez pas que le simple redémarrage de votre routeur s'en débarrassera. Les logiciels de piratage de routeur ont été conçus pour survivre aux redémarrages.

- Téléchargez toutes les mises à jour du microprogramme de votre routeur à partir du site Web du fabricant. Ensuite, signalez le piratage au Centre de plaintes contre la criminalité sur Internet.

CONNAISSEZ-VOUS VOTRE ROUTEUR ?

RÉFÉRENCES:

How Long Does a Router Last, and How Do You Know When to Upgrade? How Long Does a Router Last, and How Do You Know When to Upgrade? (msn.com)

Your router's security stinks: Here's how to fix it https://www.tomsguide.com/us/home-router-security,news-19245.html

What Wi-Fi Router Specs Are the Most Important? https://www.howtogeek.com/794161/what-wi-fi-router-specs-are-the-most-important/

WPA Key, WPA2, WPA3, and WEP Key: Wi-Fi Security Explained https://www.freecodecamp.org/news/wifi-security-explained/

More Secure Wi-Fi: What Is WPA3, and How to Set it Up on Your Router
https://www.pcmag.com/explainers/what-is-wpa3-secure-wifi-how-to-set-it-up-on-your-router

Wi-Fi 7 Explained (vs. Wi-Fi 6/6E): The Late-2023 State of the Gradually Game-Changing Wireless Standard
https://www.msn.com/en-us/news/technology/wi-fi-7-explained-vs-wi-fi-66e-the-late-2023-state-of-the-gradually-game-changing-wireless-standard/ar-AA1k9oLC

Which Wi-Fi standard is right for you? Wi-Fi 6, Wi-Fi 6E & Wi-Fi 7 explained https://www.msn.com/en-us/news/technology/which-wi-fi-standard-is-right-for-you-wi-fi-6-wi-fi-6e-wi-fi-7-explained/ar-AA1fCxdC

Wi-Fi 7 is here to make your internet faster—here's what you need to know Wi-Fi 7 is here to make your internet faster—here's what you need to know (msn.com)

Wi-Fi 7 Is Super Fast and Reliable but Needs More Time to Mature **https://www.lifewire.com/wi-fi-7-fast-needs-to-mature-8426689**

How to Enable a Guest Access Point on Your Wireless Network https://www.howtogeek.com/153827/how-to-enable-a-guest-access-point-on-your-wireless-network/

How to Hide a Router Without Blocking the Signal How to Hide a Router Without Blocking the Signal (msn.com)

How to Set Up VPN on a Router How to Set Up VPN on a Router (msn.com)

CONNAISSEZ-VOUS VOTRE ROUTEUR ?

WEP (Wired Equivalent Privacy)
WPA (Wi-Fi Protected Access)
WPS (Wi-Fi Protected Setup)

Questions