SÉCURISER SON RÉSEAU WI-FI

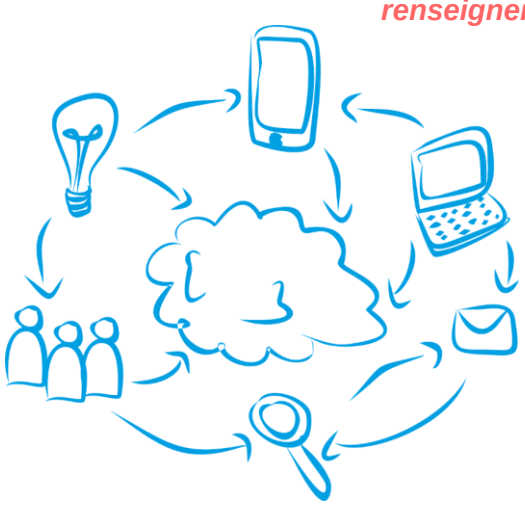
? Pourquoi sécuriser son réseau Wi-Fi ?

La technologie Wi-Fi permet d'accéder à un système d'information **à distance** et **sans fil**, dès lors que l'on est à portée du réseau émis par la borne Wi-Fi. Ce réseau est donc plus vulnérable aux attaques, puisqu'il est théoriquement accessible à tous. Un criminel numérique pourrait dès lors :

- Changer les paramètres de votre réseau et de vos ordinateurs
- Écouter l'ensemble de vos communications
- Accéder à votre Webcam ou à votre réseau de vidéosurveillance
- Intercepter des données intéressantes (mot-de-passe, coordonnées bancaires, historique compromettant ou données pouvant le renseigner sur vos habitudes ou votre style de vie, facilitant l'usurpation d'identité)
- Utiliser votre accès internet à des fins illégales

Pour vous protéger, voici quelques conseils pour sécuriser au mieux votre réseau Wi-Fi. **Veuillez noter que la plupart de ces actions de paramétrage pourront être menés depuis l'espace client mis à votre disposition par votre fournisseur d'accès à internet, ou (le cas échéant) directement depuis votre routeur (box)**.

N'hésitez pas à contacter le service client de votre fournisseur d'accès à internet pour tout renseignement à ce sujet !



CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES

dpd@cdg30.fr
04 66 38 86 86

Choisir le bon protocole de chiffrement

- Lors de la configuration du réseau Wi-Fi, vérifiez que le réseau utilise bien le **protocole WPA3-PSK** (ou à défaut, le protocole WPA2-PSK)
- Ne jamais utiliser le protocole WEP, devenu obsolète

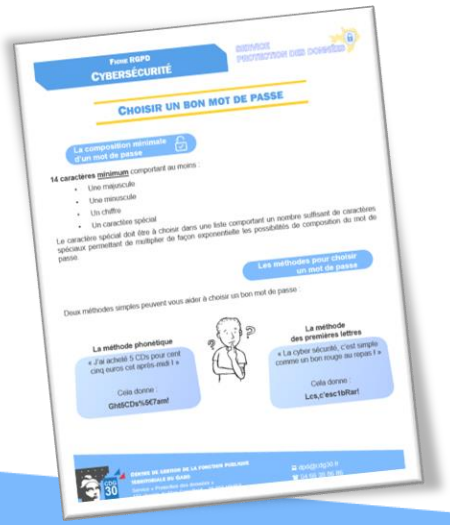
Activer le pare-feu de votre box

- Cette activation est possible, la plupart du temps, via l'espace client de votre fournisseur d'accès à internet

Choisir une clé de connexion sécurisée

- Cette « clé » correspond au mot-de-passe à taper pour se connecter au réseau Wi-Fi. Celle-ci doit impérativement être composée **au moins de 12 caractères dont** :
  - 1 chiffre
  - 1 lettre majuscule
  - 1 lettre minuscule
  - 1 caractère spécial
- Le caractère spécial doit être issu d'une liste de caractères spéciaux suffisamment importante, afin d'augmenter de manière exponentielle les possibilités de mots-de-passe
- De préférence, privilégiez une clé n'ayant aucun sens logique pouvant être deviné facilement

Afin de vous aider, rapportez vous à la fiche RGPD « choisir un bon mot de passe »


Fiche RGPD
CYBERSÉCURITÉ
CHOISIR UN BON MOT DE PASSE
La composition minimale d'un mot de passe
14 caractères minimum comportant au moins :
Une majuscule
Une minuscule
Un chiffre
Un caractère spécial
Le caractère spécial doit être à choisir dans une liste comportant un nombre suffisant de caractères spéciaux permettant de multiplier de façon exponentielle les possibilités de composition du mot de passe.
Les méthodes pour choisir un mot de passe
Deux méthodes simples peuvent vous aider à choisir un bon mot de passe :
La méthode phonétique
« J'ai acheté 5 CDs pour cent cinq euros cet après-midi ! »
Cela donne :
Ght5CDs%5€7ami!
La méthode des premières lettres
« La cyber sécurité, c'est simple comme un bon rouge au repas ! »
Cela donne :
Lcs,c'esc1bRar!

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86

Désactiver le réseau lorsqu'il est inutilisé

- Un réseau Wi-Fi actif reste une porte d'entrée potentielle pour tout criminel numérique. Si ce réseau n'est pas utilisé, désactivez-le

N'utilisez pas de réseau Wi-Fi « public »

- Evitez au maximum de vous connecter aux réseaux publics (gares, hôtels, restaurants, trains, etc.), très peu sécurisés
- De manière générale, ne vous connectez pas à un réseau sur lequel vous n'avez pas la maîtrise des paramètres de sécurité (amis, voisins, etc.)

Ne divulguez la clé de connexion à personne

- Ne la divulguez qu'à des personnes de confiance et ne la divulguez pas aux invités occasionnels
    - Si possible, installez un outil permettant de générer un identifiant de connexion unique pour tout visiteur qui garantisse son identité et conserve une trace de chaque accès au réseau
- Changez la clé de connexion régulièrement

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86