



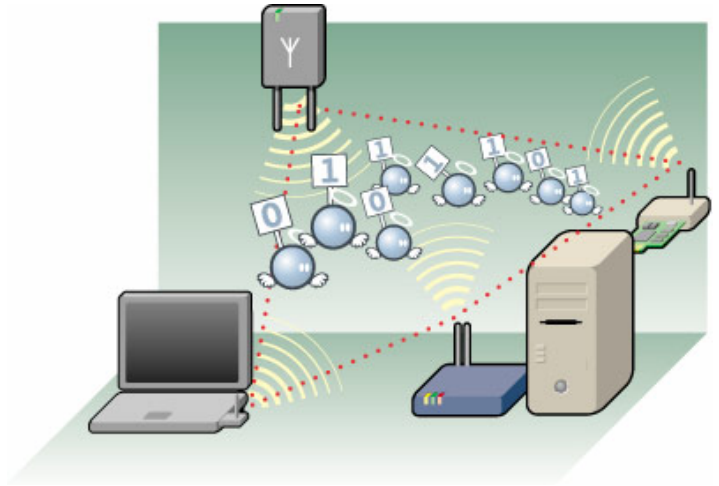
WIFI SÉCURISÉ

Pour plus de sécurité, adoptez les réflexes CASES !

Table des matières

1. Évaluez vos risques !
2. Gérez en bon père de famille !
3. Ayez le bon réflexe !

Vous offrez un accès Internet à vos clients. C'est un bon argument pour vos clients, adeptes du web ou même du web 2.0, de passer quelques moments de plus chez vous, respectivement de repasser plus régulièrement. Mais offrir un service, même s'il est gratuit, **engage votre responsabilité**. La démarche exposée ci-dessous, vous aide à mieux comprendre et à assumer correctement les responsabilités légales qu'engendre un tel service.



1

Évaluez vos risques !

Évaluez les **trois types de risques** liés à la mise en place d'une infrastructure WiFi :

1. Un client pourrait utiliser votre connectivité, donc votre identité pour **perpétrer des délits ou même des crimes** avec l'aide d'outils informatiques.
2. Un client, en utilisant votre connectivité, pourrait **devenir victime** d'une attaque provenant d'Internet.
3. Une personne malintentionnée, pourrait **s'infiltrer dans votre réseau de production** en passant par le réseau WiFi que vous mettez à disposition.

2

Gérez en bon père de famille !

Gérez votre infrastructure en « **bon père de famille** » afin de pouvoir démontrer que vous avez tout fait pour prévenir ces risques.

Avant de mettre en place l'infrastructure, vous devez répondre aux questions suivantes et mettre en place les mesures appropriées :

1. **Voulez-vous autoriser tout le monde à utiliser votre infrastructure ?**
 - a. Uniquement les clients qui ont acheté un service ou un bien.
 - b. Toutes les personnes qui savent capter le signal WiFi qui émane de votre infrastructure.

N'ouvrez pas votre infrastructure à tout le monde !

2. Voulez-vous restreindre l'accès vers des contenus illicites ?

- a. L'accès vers Internet est-il entièrement ouvert ?
- b. L'accès vers Internet est-il filtré ?

Limitez l'accès à des contenus illicites comme notamment les contenus pédopornographiques, racistes, révisionnistes couverts par les articles 384, 385bis et 454 du Code pénal.

3. Voulez-vous restreindre l'utilisation de votre connectivité aux services WWW et courrier électronique ?

- a. Votre client peut-il utiliser tout type de logiciel sur votre infrastructure (Peer-to-Peer, outils d'attaque informatiques, ...)?
- b. Voulez-vous limiter la possibilité d'usage d'outils illicites en utilisant un firewall ?

Limitez au maximum la possibilité d'utiliser votre infrastructure à des fins répréhensibles par la loi comme notamment le peer2peer ou les outils d'attaque.

4. Voulez-vous offrir un service additionnel à vos clients ?

- a. Protection avec un pare-feu.
- b. Protection avec un logiciel antivirus.

Protégez vos clients !



Ayez le bon réflexe !

En répondant à ces questions et en mettant en place une infrastructure appropriée, **vous pouvez vous protéger vous-mêmes ainsi que vos clients contre certains risques.**

Démontrez à votre clientèle via le label « WiFi sécurisé suivant les réflexes CASES » que vous gérez votre service en bon père de famille et que vous offrez un service de qualité et bien sécurisé.

La labellisation constitue une démarche volontaire. **Les audits ainsi que l'inscription au registre sont faits de façon gratuite par le service CASES** du Ministère de l'Économie et du Commerce extérieur. Le processus de labellisation se déroule en quatre étapes :

- * Étape 1 - Demande de labellisation
- * Étape 2 - Contrôle préalable
- * Étape 3 - Délivrance du label
- * Étape 4 - Contrôles de suivi annuels

Veuillez consulter le site de CASES sous <http://www.cases.public.lu/fr/pratique/label/labellisation/index.html>



Pour de plus amples informations, veuillez nous contacter sous: label@cases.lu



MINISTÈRE DE L'ÉCONOMIE
ET DU COMMERCE EXTÉRIEUR
Direction du Commerce électronique
et de la Sécurité informatique