Hadopi

BONNES PRATIQUES A L'EGARD DE STRUCTURES METTANT UNE CONNEXION À DISPOSITION D'UN PUBLIC

Dans le cadre des lois dites « Hadopi », le titulaire d'un abonnement à internet, qu'il soit une personne physique ou une personne morale, peut recevoir des avertissements de l'Hadopi car il a l'obligation de veiller à ce que sa connexion ne fasse pas l'objet d'une utilisation illicite.

N'importe quelle structure peut voir sa responsabilité engagée même si sa connexion est partagée avec un public et que plusieurs utilisateurs se servent de cette connexion à internet.

Ce document est composé d'outils pratiques qui permettront, s'ils sont combinés, de limiter les risques d'utilisation frauduleuse de la ligne internet d'une structure qui met à disposition sa connexion à des utilisateurs.

Au préalable, les bonnes questions à se poser :

- Qui sont les utilisateurs autorisés à se connecter à mon réseau Internet ?
- Comment les utilisateurs se connectent-ils à mon réseau (Wi-Fi, Filaire) ?
- Quelles mesures ont été mises en place pour limiter la connexion à mon accès aux seuls utilisateurs autorisés ?
- Quelles mesures ont été mises en place pour prévenir l'utilisation de mon accès à internet à des fins de contrefaçon ?
- Ai-je sensibilisé mes utilisateurs sur la bonne manière d'utiliser la connexion à internet que je mets à leur disposition ?
- Quelles solutions et quels outils sont à ma disposition pour prévenir de nouveaux manquements ?

I. LA SECURISATION DES ORDINATEURS

❖ *La vérification de l'installation de logiciels de partage et leur désinstallation*

Un logiciel de type « eMule », « uTorrent », « Vuze », « LimeWire » ou autre logiciel de partage (pair à pair) peut être actif sur un ordinateur de votre structure. S'il n'est pas désactivé, ce type de logiciel peut mettre à disposition automatiquement des fichiers téléchargés (comme des œuvres cinématographiques ou musicales protégées par un droit d'auteur).

En effet, un logiciel de partage est utilisé, le plus souvent, à la fois pour le téléchargement d'un fichier (consultation), mais il met aussi à disposition le fichier pour d'autres internautes qui utilisent le même logiciel (mise en partage).

Afin d'éviter la mise en partage automatique d'œuvres protégés par un droit d'auteur, il est possible de désinstaller un logiciel de partage. Sur Windows cela peut se faire en utilisant le module de gestion des programmes (rubriques « panneau de configuration » et « ajout/suppression de programmes »).

Accédez à la fiche pratique sur la désinstallation de ces logiciels, disponible sur le site internet de l'Hadopi www.hadopi.fr au sein de la rubrique « Sensibilisation > Les fiches pratiques ». Afin de mieux comprendre la marche à suivre pour opérer la désinstallation de ces logiciels, une vidéo est également en ligne dans la rubrique « Sensibilisation > Les vidéos tutos ».

❖ *Le paramétrage des ordinateurs avec les fonctionnalités « administrateur » et « utilisateur »*

Dans le cas où des ordinateurs sont partagés entre plusieurs utilisateurs au sein de la structure, il est recommandé de créer des comptes secondaires pour les utilisateurs.

Le compte « administrateur » est le compte principal de l'ordinateur qui gère notamment l'installation des programmes, comme les logiciels de partage, et les opérations de maintenance de l'ordinateur.
Le compte « utilisateur » n'a que des possibilités limitées, il permet surtout de disposer de son propre espace personnel.

(Pour plus d'informations, voir la fiche pratique *Mon ordinateur, quelle maintenance et quelle sécurité ?*).

II. LA SECURISATION DU WIFI

N.B. : toutes les informations sur la box et son paramétrage sont disponibles sur le site internet de l'Hadopi dans une fiche pratique *Qu'est-ce qu'une box ? Comment paramétrer sa box ?*

❖ *La clé de chiffrement pour le boîtier de connexion*

La sécurisation de l'accès à internet permet de limiter l'accès aux seules personnes autorisées qui détiennent le code. La fiabilité de la sécurité de l'accès peut être augmentée en utilisant une clé WPA2 pour prévenir la connexion de personnes extérieures à la structure.

Cette clé est en principe générée une première fois lors de la première installation de la box. Elle peut ensuite être personnalisée et modifiée directement par la personne gérant le réseau.

(Pour plus d'informations, voir la fiche pratique *Qu'est-ce que le Wifi et comment bien l'utiliser ?*)

❖ *La visibilité du réseau wifi*

Il est important de ne pas conserver un nom de réseau sans fil wifi (SSID) générique et proposé automatiquement par défaut par le fournisseur d'accès. Il est recommandé que le SSID ne soit pas trop explicite par rapport à une activité professionnelle ou une information personnelle.

Il est possible de changer manuellement le SSID dont la diffusion pourra être masquée grâce l'option disponible sur votre boitier de connexion. Celui-ci n'apparaitra pas spontanément comme un réseau wifi disponible auquel un utilisateur ponctuel pourrait se connecter.

III. LA SECURISATION PAR FILTRAGE

❖ *Filtrage de contenus*

Des solutions logicielles permettent de filtrer les types de contenus auxquels les utilisateurs pourraient avoir accès sur le web. Même si aucune ne peut être fiable à 100 %, il s'agit d'une mesure de précaution. Il est possible d'appliquer des limites horaires portant tout aussi bien sur l'utilisation de tel ou tel programme en particulier (navigateur internet, Skype, jeu vidéo, etc.) que sur celle de la connexion internet ou de l'ordinateur lui-même. Ce type de logiciels fonctionne selon trois principes distincts :

- L'interdiction de mots ou formules clés établis dans une liste, tels que sexe par exemple. Cette méthode ne saurait néanmoins être totalement efficace, du fait, notamment, des sites en langue étrangère ou bien des cas où textes et visuels ne correspondent pas.

- La liste noire, qui consiste à mettre à jour à chaque connexion une liste de sites interdits par le logiciel. Là aussi l'efficacité n'est qu'approximative, car des sites sensibles sont lancés chaque jour sur le réseau.
- La liste blanche est une solution plus sûre mais très restrictive, où seuls les sites autorisés seront accessibles. La liste de ces derniers peut être modifiée à votre gré.

Pour plus d'efficacité, il peut être intéressant d'utiliser une solution où sont combinés interdiction de termes clés et liste noire.

Pour terminer :

- Toutes ces recommandations seront efficaces si un bon paramétrage est opéré et mis à jour régulièrement et qu'une maintenance sécurité est effectuée au quotidien. À ce sujet, une fiche pratique *Mon ordinateur quelle maintenance et quelle sécurité ?* est consultable sur le site de l'Hadopi.

- Ces bonnes pratiques seront d'autant plus efficaces si elles sont accompagnées d'une sensibilisation accrue des utilisateurs. Il est possible de trouver sur le site internet de l'Hadopi des outils de prévention et de sensibilisation à destination des utilisateurs des connexions internet. Il suffit de se rendre sur la page dédiée aux professionnels « Réagir à la réception d'une recommandation » puis de sélectionner le type de structure afin de faire apparaître les documents adaptés.

Pour information, un ensemble de fiches pratiques sur internet, les questions techniques, l'offre légale ou encore l'identité numérique est accessible sur le site de l'Hadopi.