Hadopi

BONNES PRATIQUES A L'EGARD DES STRUCTURES METTANT LEUR CONNEXION A DISPOSITION D'UN PUBLIC

Dans le cadre des lois Hadopi, le titulaire d'un abonnement, qu'il soit une personne physique ou une personne morale, peut voir sa responsabilité engagée si sa connexion à internet est utilisée à des fins de contrefaçon par lui-même ou par un tiers.

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.

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. 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, vous pouvez désinstaller le 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 »).

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

Dans le cas où des ordinateurs sont partagés entre plusieurs utilisateurs au sein de votre 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 ?* sur le site de l'Hadopi).

II. LA SECURISATION DU WIFI

❖ *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.
Si ce n'est pas déjà le cas au sein de votre structure, la fiabilité de la sécurité de l'accès peut être augmentée en utilisant une clé WPA2 pour prévenir la connexion de personnes extérieures à votre 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 ?* sur le site de l'Hadopi).

❖ *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 votre 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.

❖ *Application d'un filtrage applicatif*

Le filtrage applicatif est une analyse protocolaire qui peut permettre, notamment, de filtrer le partage *via* des logiciels pair à pair.

Le pare-feu applicatif permet de récupérer tous les paquets d'une connexion et d'en faire une analyse en profondeur. Le pare-feu peut être configuré pour reconnaître les protocoles et connexions légitimes. Le mécanisme de filtrage rejettera toutes les connexions qui ne sont pas conformes aux protocoles autorisés. Il consiste ainsi à repérer et bloquer tous les flux d'une certaine nature (par exemple bloquer le protocole BitTorrent empêche de télécharger des fichiers à travers ce type de logiciel pair à pair).

❖ *Application d'un filtrage par port*

Certains logiciels ou services de partage utilisent un port dont le numéro est défini par avance. Un filtrage peut être mis en place sur ce port afin que, l'application ou le service soit bloqué(e).

Les dispositifs pare-feu sont capables de filtrer les communications selon le port utilisé. Il peut être conseillé de bloquer tous les ports qui ne sont pas indispensables à la simple navigation internet et/ou aux services de messagerie (selon la politique de sécurité de la structure retenue).

N.B. : 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.
(voir à ce sujet la fiche pratique *Mon ordinateur quelle maintenance et quelle sécurité ?* sur le site de l'Hadopi).

De plus, ces bonnes pratiques seront d'autant plus efficaces si elles sont accompagnées d'une sensibilisation accrue des utilisateurs.

Pour votre 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 à la rubrique *Fiches pratiques*.