LE GUIDE PRATIQUE DES PROFESSIONNELS

Protéger votre connexion internet des utilisations illicites et sensibiliser ses utilisateurs

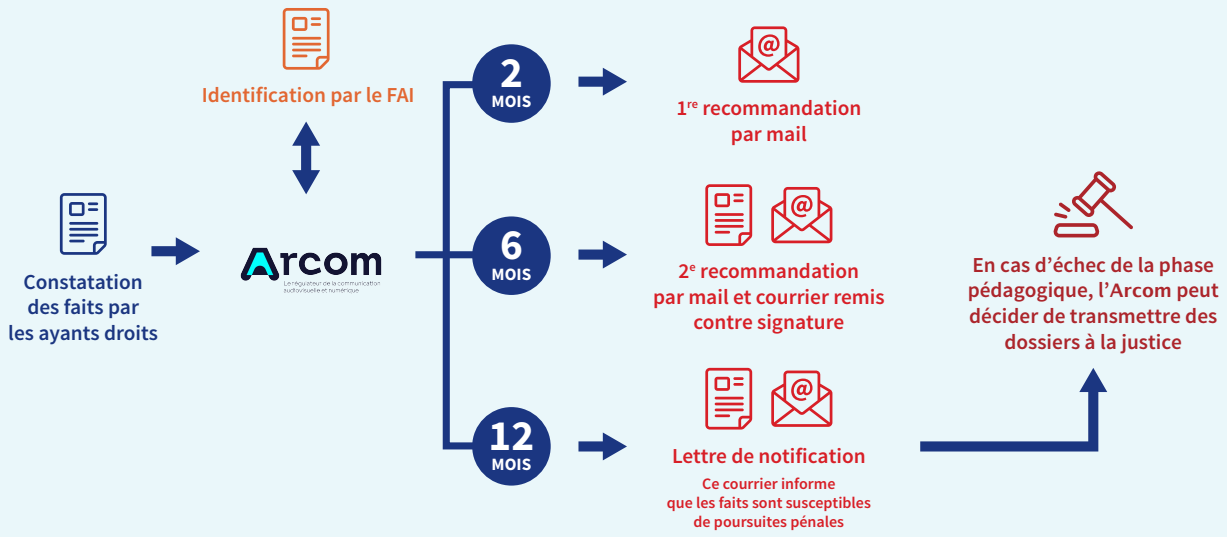
Vous êtes une structure professionnelle (administration, société, association, collectivité locale, hôtel, camping, bar, restaurant…) et vous êtes titulaire d'un abonnement à internet ? Vous accueillez aussi du public et vous lui mettez à disposition cet accès à internet ? Dans le cas d'une utilisation illicite de votre connexion internet, votre responsabilité pénale peut être engagée.
Ce guide vous propose les bonnes pratiques pour sécuriser votre accès internet et éviter son utilisation à des fins illicites.

L'obligation légale de sécuriser votre connexion à internet

Les professionnels qui disposent d'une connexion à internet sont soumis, au même titre que les particuliers, à l'obligation de sécuriser leur connexion à internet afin qu'elle ne soit pas utilisée pour télécharger ou mettre à disposition sur internet des œuvres protégées par le droit d'auteur (film, musique, série télévisée). Un professionnel qui met sa connexion à disposition de ses salariés, de ses clients ou du public peut ainsi voir sa responsabilité engagée, en tant que titulaire de l'abonnement.

LA PROCÉDURE DE RÉPONSE GRADUÉE

La procédure de réponse graduée était mise en œuvre par l'Hadopi à compter de 2009 et par l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), depuis le 1er janvier 2022. Cette procédure consiste à envoyer des avertissements aux titulaires d'un abonnement internet lorsque celui-ci a été utilisé pour mettre à disposition sur des réseaux pair à pair des œuvres culturelles sans en avoir l'autorisation des ayants droit. Si à l'issue des différents avertissements, les faits persistent, l'Hadopi peut saisir le procureur de la République. Dans ce cas, le professionnel titulaire de la connexion risque une contravention pour négligence caractérisée* pour laquelle la peine maximale encourue est de 7 500 € pour les personnes morales.



LES BONNES QUESTIONS À VOUS POSER

1. Quels sont les utilisateurs autorisés à se connecter à mon réseau internet ?
2. Comment les utilisateurs se connectent-ils à mon réseau (WiFi, Filaire, ordinateur fourni par mes soins, équipement personnel de l'utilisateur…) ?
3. Quelles mesures ai-je mis en place pour limiter la connexion à mon accès internet aux seuls utilisateurs autorisés ?
4. Quelles mesures ai-je mis en place pour prévenir l'utilisation de mon accès à internet à des fins de contrefaçon ?
5. Ai-je sensibilisé mes utilisateurs à la bonne manière d'utiliser la connexion à internet que je mets à leur disposition ?
6. Quelles solutions et quels outils sont à ma disposition pour prévenir de nouveaux manquements ?

LES BONS RÉFLEXES QUE VOUS DEVEZ AVOIR

Mise à disposition d'ordinateurs

- Désinstaller les logiciels pair à pair
- Paramétrer les ordinateurs en mode Administrateur/utilisateur
- Installer une clé de chiffrement sur le boîtier de connexion
- Masquer le réseau WiFi

Mise à disposition de connexion WiFi

- Mettre un pop-in informatif lors de la connexion
- Sensibiliser mes publics par la diffusion d'une clause de bonne conduite ou d'une charte d'utilisation
- Installer une clé de chiffrement sur le boitier de connexion
- Appliquer un filtrage par port
- Appliquer un filtrage applicatif
- Appliquer un filtrage de contenus

▸ Comment sécuriser les ordinateurs que vous mettez à disposition ?

VOUS DEVEZ VÉRIFIER ET DÉSINSTALLER LES LOGICIELS PAIR À PAIR S'ILS SERVENT UNIQUEMENT AUX TÉLÉCHARGEMENTS ILLÉGAUX

Les logiciels ou applications pair à pair (peer to peer, comme « uTorrent », « BitTorrent », « Azureus », « Transmission » etc.) peuvent être actifs sur un ordinateur de votre structure, mis à disposition des salariés ou du public. Ils sont paramétrés pour mettre à disposition automatiquement, dès que l'ordinateur se connecte à internet, des fichiers précédemment téléchargés.

En effet, un logiciel de partage sert, la plupart du temps, à la fois au téléchargement d'une œuvre (afin de la consulter), mais aussi à sa mise à disposition pour d'autres internautes qui utilisent le même logiciel (ce qu'on appelle aussi la mise en partage de l'œuvre). Afin d'éviter la mise en partage automatique d'œuvres protégées par un droit d'auteur, et si un tel logiciel n'est utilisé que dans ce but, nous vous invitons à le désinstaller de vos postes informatiques / ou d'inviter les utilisateurs de votre connexion à les désactiver ou à les désinstaller de leur ordinateur avant de se connecter à votre réseau.

Accéder au tutoriel sur le site Arcom ↗

VOUS POUVEZ PARAMÉTRER LES ORDINATEURS EN MODE ADMINISTRATEUR/UTILISATEUR

Il est recommandé de créer des profils d'utilisateurs distincts sur les ordinateurs mis à disposition du public, et de réserver le profil « administrateur » au compte principal de l'ordinateur qui gère notamment l'installation des programmes et les opérations de maintenance de l'ordinateur. Le compte « utilisateur » n'a dans ce cas que des possibilités limitées : Par exemple, il ne permet pas en général d'installer des programmes.

▸ Comment sécuriser votre accès internet ?

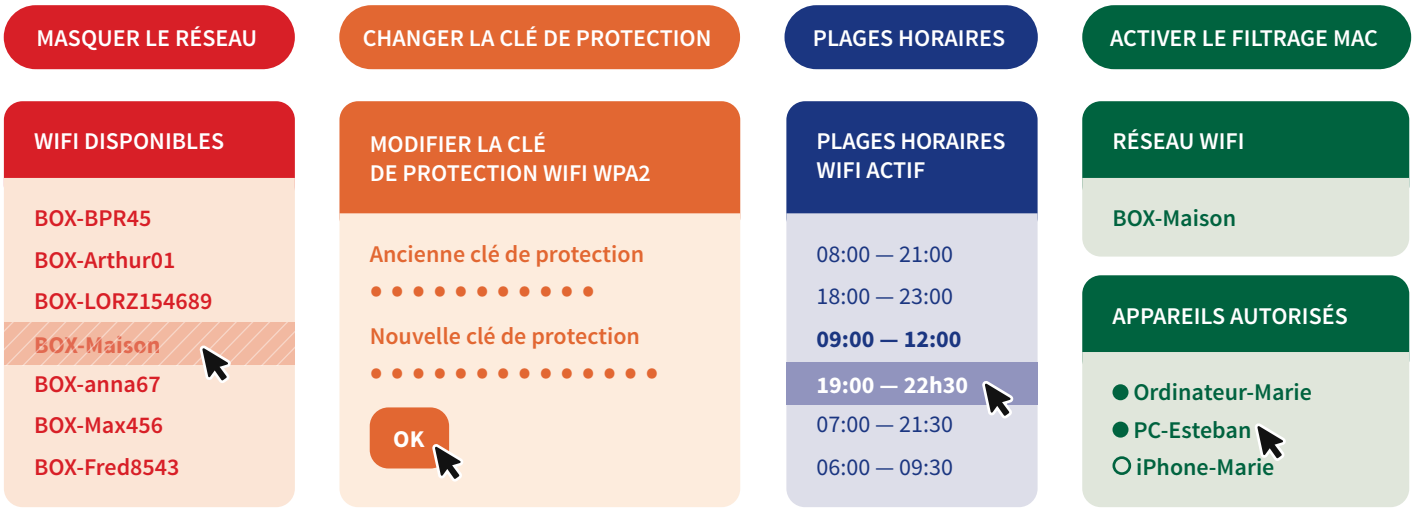
VOUS POUVEZ INSTALLER UNE CLÉ DE CHIFFREMENT

Si ce n'est pas déjà le cas, vous pouvez augmenter la fiabilité de la sécurité de votre accès en installant une clé WPA2. Vous indiquerez ainsi que l'accès à internet est protégé par un code.

VOUS POUVEZ PARAMÉTRER LA BOX

En tant que professionnel, il se peut que vous partagiez votre réseau avec un public en communiquant le mot de passe WiFi de votre boîtier de connexion (box) à des locataires, des adhérents d'une association ou des salariés par exemple. Il est alors possible de prendre des mesures pour contrôler l'utilisation de la box mise à disposition de tiers en la paramétrant via l'interface de celle-ci. Vous pouvez notamment désactiver le WiFi communautaire, masquer le réseau WiFi pour des utilisateurs externes (c'est-à-dire autres que les personnes à qui vous avez autorisé la connexion) ou encore définir des plages horaires pendant lesquelles le WiFi du boitier de connexion sera activé.

Accéder au tutoriel sur le site Arcom ↗



MASQUER SON RÉSEAU WIFI

Cela permet à votre boitier de connexion de ne plus être visible et ainsi de restreindre les connexions extérieures sur votre réseau. Dans la plupart des panneaux de configuration des box il faut cliquer sur l'onglet Diffusion du SSID, le désactiver puis valider les changements.

COMMENT RÉGÉNÉRER SA CLÉ DE PROTECTION WPA2 (WIFI PROTECTED ACCESS)

Pour se connecter au boitier de connexion via le WiFi, l'utilisateur devra renseigner la clé (suite de caractères alphanumériques) dans l'interface de son appareil.

Deux possibilités de récupérer une clé :

1. Un numéro à lire sur une étiquette boitier de connexion et à reporter sur le « point d'accès » du réseau.
2. Un bouton (physique ou virtuel), à la fois sur le boitier de connexion et le point d'accès du réseau.

PLANIFICATEUR WIFI

La gestion de cette option permet de définir des règles différentes pour chaque jour de la semaine ou pour une période d'absence prolongée (congés). Dans le cadre du contrôle parental, vous pouvez ainsi gérer les plages horaires de connexion Internet sur les ordinateurs, tablettes, téléphones portables de votre foyer.

LE FILTRAGE MAC (LISTE NOIRE ET LISTE BLANCHE)

Le filtrage MAC permet de renforcer la sécurité de votre réseau. Par défaut, cette fonction est désactivée. L'activation du filtrage MAC permet d'autoriser uniquement les périphériques dont les adresses Mac sont renseignées à se connecter au réseau WiFi (liste blanche) ou d'interdire la connexion de certains appareils spécifiquement désignés (liste noire).

VOUS POUVEZ APPLIQUER DES MESURES DE FILTRAGE SUR VOTRE BOX

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 soient bloqués.

FILTRAGE APPLICATIF

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

FILTRAGE DE CONTENUS ET D'URLS

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.

▸ Comment sensibiliser vos utilisateurs ?

Il n'est pas possible de sécuriser de manière absolue un réseau WiFi, mais il est possible de sensibiliser vos utilisateurs (publics, administrés, etc.) à une utilisation respectueuse de l'accès internet que vous proposez grâce à :

L'affichage sur l'écran d'un message de sensibilisation lors de l'accès au WiFi, sous forme de « pop-in ».

L'élaboration d'une charte informatique ou l'insertion d'une clause dans votre charte ou le contrat de location (dans le cas de professionnels de l'hébergement).

L'affichage d'un message de sensibilisation dans les lieux de passage.

L'organisation de réunions ou ateliers pour sensibiliser de visu les utilisateurs, notamment lors de la transmission du mot de passe.

Vous pouvez retrouver les fiches pratiques, les vidéos tutorielles, le livret de sensibilisation à télécharger sur arcom.fr

Autorité de régulation de la communication audiovisuelle et numérique
39/43 quai André Citroën 75015 PARIS