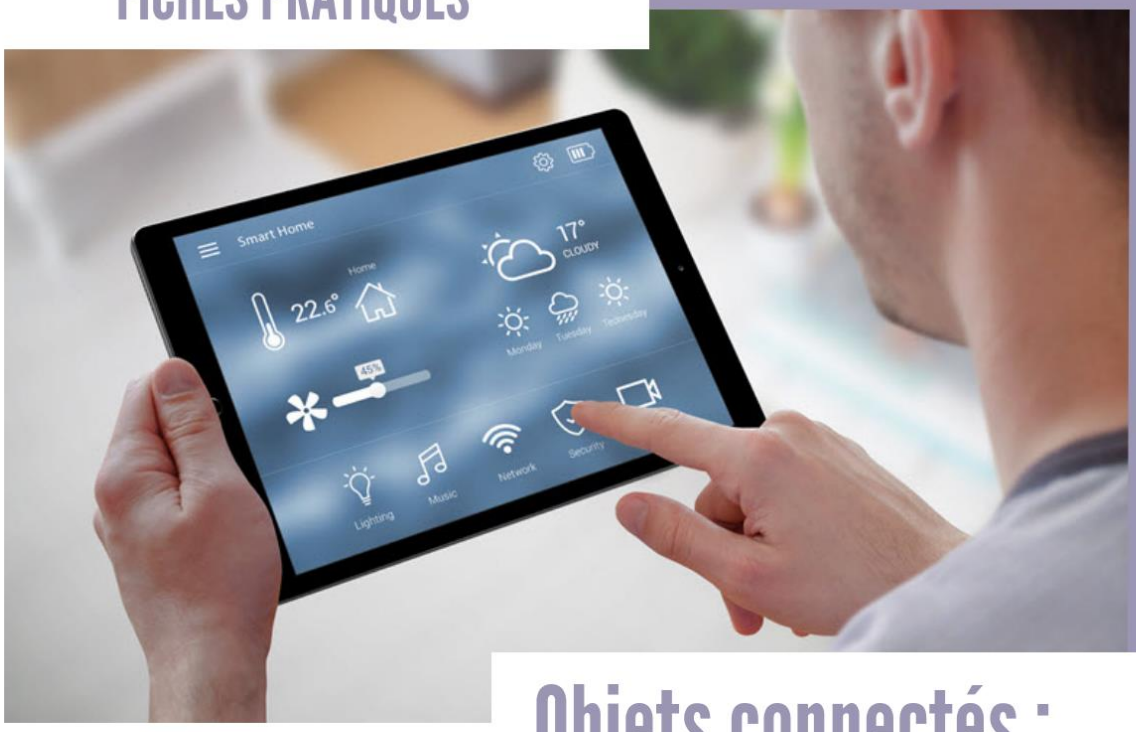
FICHES PRATIQUES



Objets connectés :
Les risques à connaître

Contrôler sa glycémie sur sa montre, mesurer ses performances au golf ou au tennis sur son téléphone, déclencher à distance la climatisation de son domicile…, les domaines d'application des objets connectés sont sans limite. Mais attention à bien sécuriser les informations qui transitent sur ces appareils !

Qu'est-ce qu'un objet connecté ?

Il s'agit d'un matériel électronique qui peut communiquer avec un smartphone, une tablette tactile, une montre, un ordinateur ou une télévision. Communiquer, cela signifie qu'il peut envoyer et recevoir des informations, par le biais d'une liaison sans fil, Bluetooth ou Wifi.

Un marché en plein essor…

Selon une étude du cabinet GFK, en 2016, les Français ont acheté plus d'un million d'objets connectés (*smartwatches* et *trackers* d'activité), en hausse de 28 % par rapport à 2015. Le marché atteint ainsi 253 millions € à + 20 %. Si le chiffre d'affaires généré est légèrement en deçà des prévisions, celui-ci s'explique en partie par une légère baisse de prix moyen des montres connectés (-7 %) et des bracelets de sport (-9 %).

En termes de parc installé, le bassin parisien concentre 42 % des possesseurs d'objets connectés, tous types confondus. Cela s'explique par une plus grande offre de magasins spécialisés, ou dotés de rayons spécifiques, et une population plus urbaine à fort pouvoir d'achat.

… mais encore hétérogène

Fait notable : la notoriété des objets connectés n'a pas augmenté depuis l'année dernière. Ainsi, les bracelets d'activité affichent un (modeste) score de notoriété de 36 % en 2016, proportion qui monte à près d'un consommateur sur deux pour la *smartwatch* (48 %).

Le développement de ces produits ne serait donc pas homogène. Toujours selon GFK, les objets connectés représenteraient à peine 1 % du chiffre d'affaires de l'électroménager et seulement 5 % du marché de la domotique.

Un niveau d'équipement faible

Dans une autre enquête, réalisée par l'IFOP, seulement 22 % des Français interrogés déclaraient posséder au moins un objet connecté : bracelet pour mesurer l'activité ou la condition physique (5 %), montre connectée (5 %), thermostat connecté (8 %), volets roulants (4 %), aspirateur (3 %), balance connectée (5 %), réfrigérateur (2 %).

De même, selon une étude du cabinet Xerfi sur le marché des objets connectés, les montres et *trackers* d'activités ne représenteraient que 1 % des dépenses high-tech des Français, loin derrière les smartphones et autres tablettes.

Les domaines d'application

La santé : avec un bracelet connecté, une balance ou un tensiomètre, non seulement vous pouvez réaliser vos mesures à domicile, mais vous avez également la possibilité d'effectuer un suivi médical, seul ou en collaboration avec un médecin. Autre fonction à succès : la gestion du sommeil qui permet de connaitre les différentes phases de votre sommeil et, si votre appareil est doté d'une alarme silencieuse, d'optimiser votre réveil.

Le sport : grâce aux *trackers* d'activité, vous pouvez comptabiliser les kilomètres courus ou marchés et synchroniser ces résultats sur votre smartphone ou votre tablette. Certains appareils équipés d'un GPS sont plus particulièrement dédiés aux amateurs de running. Il existe aussi des capteurs pour le golf ou pour le tennis, destinés à mesurer, analyser et améliorer vos performances.

Les loisirs : avec les montres connectées, vous recevez vos emails et SMS, accédez à votre musique ou vos photos et vidéos, calculez un itinéraire, etc. N'oublions pas les téléviseurs connectés qui donnent accès à des contenus multimédias, des applications de loisir ou pratiques, des renseignements sur les programmes regardés…,

La domotique et la sécurité : citons, par exemple, les caméras de sécurité, qui vous permettent de contrôler votre domicile à distance et vous alertent en cas d'intrusion, ou encore les *babyphones*, grâce auxquels vous pouvez garder un œil sur votre bout de chou en train de dormir,

Les économies d'énergie : les objets connectés permettent de connaître, régler et optimiser votre consommation énergétique. Par exemple, un thermostat connecté vous permet de régler à distance la température ambiante, d'optimiser le chauffage en fonction du moment de la journée et de votre temps de présence, etc.

Quels sont les risques ?

Le développement des objets connectés expose principalement les consommateurs à deux types de risques :

- **l'utilisation commerciale des données personnelles et les atteintes à la vie privée** : une des conséquences de ce monde de réseau et de communication est que nous laissons de plus en plus de traces numériques. Au-delà des progrès technologiques, il s'agit désormais de parvenir à garantir l'anonymat des données collectées par ces appareils ;
- **le piratage** : dès lors que se connecter à internet devient une fonction intégrante d'objets du quotidien, les concepteurs de ces équipements doivent faire face aux risques de « *cyber* » attaque.

Comment se protéger ?

- Avant l'achat d'un objet connecté, informez-vous sur ses caractéristiques, son fonctionnement, ses interactions avec les autres appareils électroniques et, le cas échéant, sur les précautions à prendre.
- Après l'achat, sécurisez bien la connexion aux autres appareils communicants, en procédant régulièrement aux mises à jour de sécurité et mises à jour logicielles. L'idée est de limiter les vulnérabilités connues qui pourraient être exploitées par des personnes ou des organisations malveillantes.
- Autre conseil de bon sens, qui vaut pour la plupart des équipements informatiques : changez fréquemment le nom et le mot de passe par défaut de chaque objet connecté.
- Pour finir, limitez l'accès de l'objet connecté aux autres appareils électroniques ou informatiques. Par exemple, si vous avez une TV connectée, vous devrez vous assurer de modifier le mot de passe par défaut et choisir un réseau personnel, sécurisé, avec une clé de protection adéquate pour le Wifi et le routeur. Même chose pour les mots de passe des services et sites internet. Il faut éviter la redondance et utiliser des mots de passe robustes (mélangeant des majuscules et des minuscules, des chiffres et des caractères spéciaux (%, #, :, $, *). N'oubliez pas de restreindre l'accès à votre réseau personnel et d'isoler son accès à internet des autres éléments connectés au réseau (il n'est pas vraiment nécessaire que votre imprimante soit connectée à votre TV, par exemple).
- Sachez enfin que la principale faille qu'exploitent les pirates est encore trop souvent l'absence de vigilance des utilisateurs. Beaucoup n'ont pas conscience des risques et n'utilisent pas de mots de passe pour protéger l'accès à distance de leurs équipements, ou se contentent de laisser les identifiants par défaut fournis par les fabricants. Vous êtes acteurs de votre sécurité !

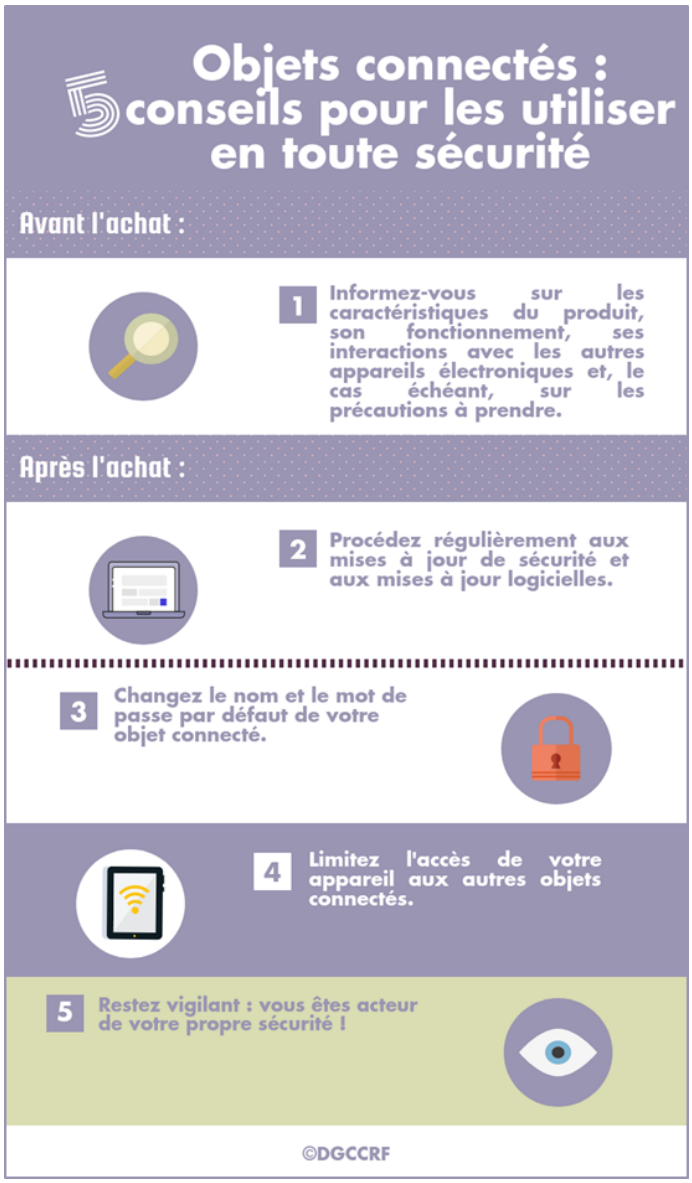
Textes de référence

Code pénal article 313-3 (tentative d'escroquerie) et article 226-1 (atteinte à la vie privée)

Liens utiles

Commission nationale informatique et libertés (CNIL)

Office central de lutte c/la criminalité et de la communication (OCLCTIC)



Les éléments ci-dessus sont donnés à titre d'information. Ils ne sont pas forcément exhaustifs et ne sauraient se substituer aux textes officiels.

Pour tout renseignement complémentaire, reportez-vous aux textes applicables et/ou rapprochez-vous d'une direction départementale de la protection des populations (DDPP) ou direction départementale de la cohésion sociale et de la protection des populations (DDCSPP).

Crédit photo : ©Fotolia