Un objet connecté (Internet of Things ou IoT en anglais) est un matériel électronique connecté directement ou indirectement à Internet, c'est-à-dire qu'il est capable d'envoyer ou de recevoir des informations par Internet. Enceintes, montres, ampoules, thermostats, téléviseurs, réfrigérateurs, jouets pour adulte ou enfant, caméras, alarmes, « baby-phones », etc., les objets connectés font aujourd'hui de plus en plus partie de notre vie numérique, tant personnelle que professionnelle, dans de nombreux domaines comme la domotique, le sport, le jeu ou bien la santé. Comme tout équipement informatique communicant, ces objets peuvent cependant présenter des vulnérabilités qui peuvent entraîner certains risques comme leur piratage ou le vol des informations personnelles qu'ils contiennent, d'autant plus qu'ils sont souvent insuffisamment sécurisés, et peuvent donc représenter le maillon faible de votre environnement numérique. Voici 10 bonnes pratiques à adopter pour utiliser au mieux vos objets connectés en sécurité.

1. Avant l'achat, renseignez-vous sur l'objet connecté

Informez-vous sur les caractéristiques de l'objet, son fonctionnement, ses interactions avec les autres appareils électroniques ou les données collectées lors de son utilisation. Vérifiez également que l'objet ne présente pas de failles de sécurité connues qui, si elles sont utilisées, pourraient permettre de prendre le contrôle de l'objet ou d'ouvrir une brèche dans votre environnement numérique et sur vos données. Pour cela, renseignez-vous auprès de sites Internet spécialisés, consultez le site Internet du fabricant ainsi que les avis de consommateurs qui peuvent fournir de précieuses informations.

2. Modifiez les mots de passes par défaut de vos objets connectés

Les mots de passe, codes PIN, etc. générés par défaut par les fabricants sont généralement trop faibles : trop peu de caractères utilisés, faciles à