Livre blanc

Bitdefender®

# Sensibilisation à la sécurité à l'ère de l'Internet des Objets

## Étude Bitdefender

# Introduction

Une bouilloire qui parle ? Un réfrigérateur qui commande vos courses pendant que vous êtes au travail ? Des plantes qui s'arrosent toutes seules ? 6,4 milliards de gadgets futuristes[1] de ce type occupent déjà une place de choix dans les foyers, qu'il s'agisse de capteurs sans fil, de caméras connectées au réseau, de prises connectées et autres ampoules Wi-Fi qui virent au bleu lorsque l'utilisateur reçoit un nouveau message sur Facebook.

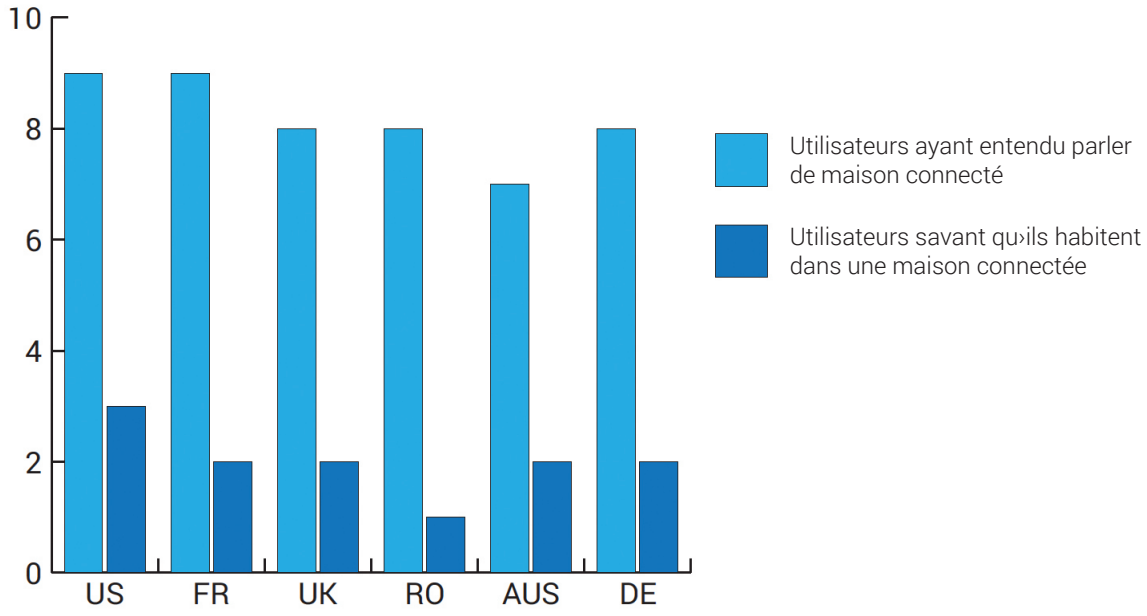
La maison du futur existe déjà et se trouve à deux pas de chez vous. Le saviez-vous ?

Ce livre blanc vise à mettre en lumière la perception qu'ont les particuliers des technologies connectées et à illustrer la manière dont les internautes américains et européens comprennent et adoptent l'IoT (Internet des Objets). Nul doute, les gens apprécient le côté innovant de ces objets connectés. Mais comment gèrent-ils les problématiques de sécurité et de confidentialité ? Sont-ils compétents, ou non, en tant qu'administrateurs des Objets de leurs maisons ?

# Principaux constats

**Les utilisateurs savent mieux ce qu'est une maison connectée que l'Internet des Objets. Moins d'un cinquième d'entre eux reconnaissent vivre dans une maison de ce type.**

Des tests visant à évaluer la notoriété de ces deux concepts clés — "l'Internet des Objets" et la "Maison Connectée" — ont permis de démontrer que les utilisateurs ont tendance à confondre les deux termes. D'après les résultats de l'étude, **la moitié des internautes résidant aux États-Unis n'ont jamais entendu parler du concept d'Internet des Objets.**




Les utilisateurs américains et français semblent tout de même mieux informés que les autres. Dans ces deux pays, 9 utilisateurs sur 10 ont entendu parler du concept de Maison Connectée. Aux États-Unis, 5 sur 10 ont entendu parler du concept de l'Internet des Objets, là où en France 6 sur 10 le connaissent. Parmi les utilisateurs qui, techniquement, vivent dans une maison connectée, seuls 3 américains sur 10 et 2 français sur 10 (17%) en sont conscients.

Au Royaume-Uni, 8 utilisateurs sur 10 ont déjà entendu parler du concept de Maison Connectée, et 5 personnes sur 10 utilisent le terme "IoT". Seuls 2 habitants sur 10 de maison connectée savent qu'ils vivent dans une maison connectée.

Un niveau de conscience similaire apparaît chez les utilisateurs roumains. 8 utilisateurs de technologie sur 10 ont déjà entendu parler du concept de Maison Connectée, tandis qu'un nombre sensiblement moins élevé (4 sur 10) n'ont qu'une vague idée de ce qu'est l'IoT. Lorsque la question leur a été posée, seul 1 habitant de maison connectée sur 10 était conscient de vivre dans une maison de ce type.

1 http://www.gartner.com/newsroom/id/3165317

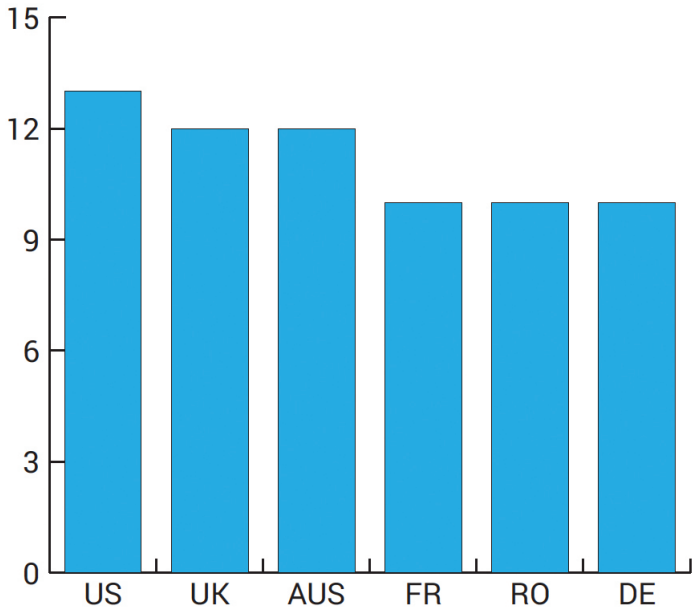
En Australie, 7 utilisateurs de technologies sur 10 ont entendu parler du concept de Maison Connectée, tandis que 5 sur 10 connaissent l'Internet des Objets. Seuls 2 habitants de maison connectée sur 10 savent qu'ils y vivent déjà.

Interrogés au sujet des concepts de l'IoT et de la Maison Connectée, 9 internautes allemands sur 10 ont affirmé avoir entendu parler de la seconde. En revanche, seuls 2 sur 10 savent qu'ils vivent dans une maison connectée.

# Possession d'appareils connectés

En moyenne, un foyer américain possède 13 appareils ou accessoires connectés. On en compte 12 au Royaume-Uni, en Australie, en Roumanie et en Allemagne tandis qu'un foyer français en possède une dizaine en moyenne.

## *Nombre d'appareils connectés par foyer*



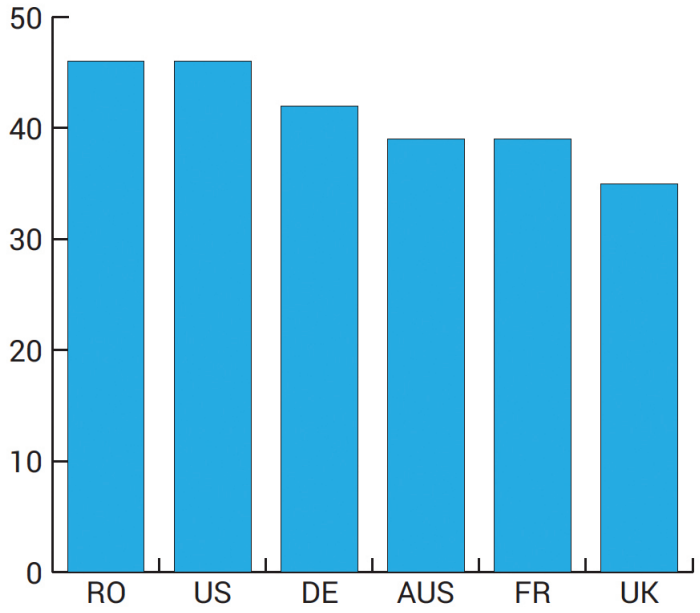

Interrogés au sujet de leur connectivité, la plupart des utilisateurs de l'IoT affirment avoir une vision plutôt claire du nombre d'appareils connectés à Internet dans leur foyer.

Dans la plupart des foyers, les principaux appareils ayant accès au réseau Wi-Fi domestique sont les smartphones, les ordinateurs sous Windows et les tablettes, suivis par les télévisions connectées et les consoles de jeux sans fil.

# Principales préoccupations liées à la sécurité

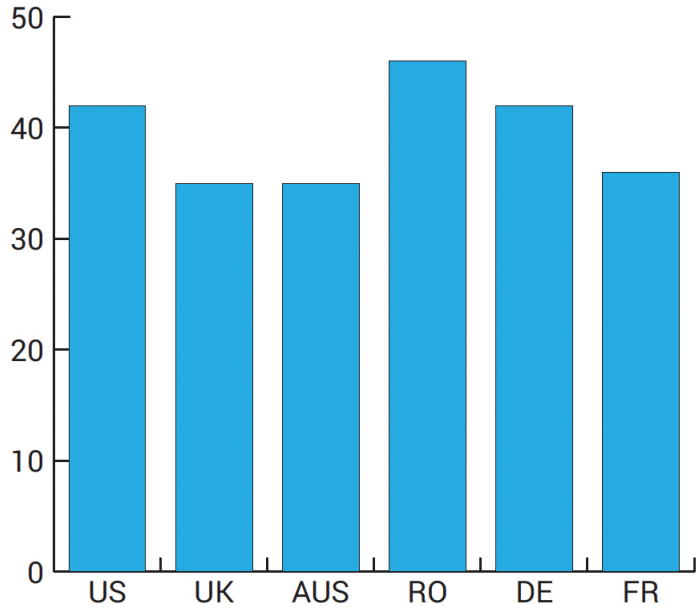
La sécurité est l'un des principaux obstacles à l'adoption de l'IoT à plus grande échelle. Une part importante des utilisateurs se préoccupent de savoir si leurs informations personnelles pourraient être dérobées ou divulguées via leurs objets connectés (46% aux États-Unis et en Roumanie, 43% en Allemagne, 39% en Australie et en France, 35% au Royaume-Uni).

*Principales préoccupations en matière de sécurité*




Deuxièmement, les utilisateurs craignent que quelqu'un prenne le contrôle de leurs appareils via Internet (42% aux États-Unis, 35% au Royaume-Uni, en Australie et en Roumanie, 45% en Allemagne et 36% en France).

*Préoccupations liées à la perte de contrôle des appareils connectés*



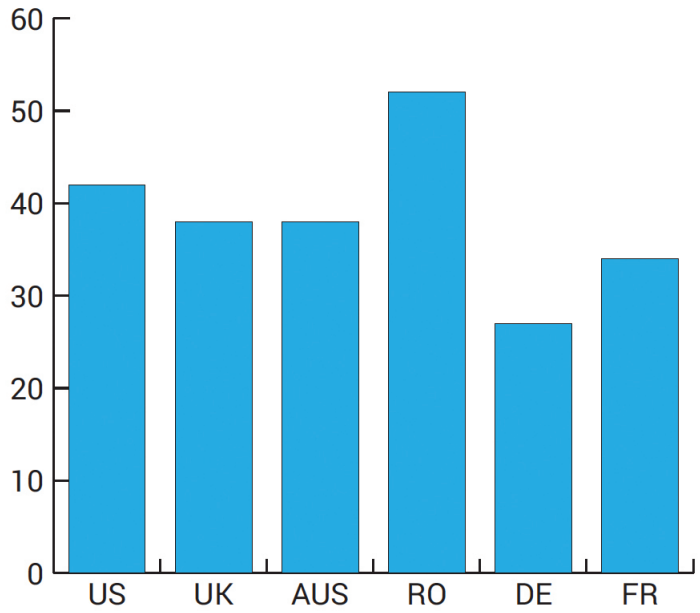
Leurs inquiétudes sont d'autant plus décuplées par des études qui mettent en évidence les dangers qui pèsent sur les appareils non sécurisés dans une maison. Récemment, les chercheurs de Bitdefender[2] ont découvert que les caméras connectées pouvaient être détournées et transformées en outils d'espionnage. Quiconque sachant tirer parti d'une faible authentification serveur est en mesure de se connecter sur les serveurs du fabricant et de s'enregistrer à la place de l'appareil original, afin d'en prendre pleinement le contrôle. Ainsi, ce pirate pourra espionner les membres d'une famille, voire même parler aux enfants à travers les appareils de surveillance présents dans leurs chambres.

"Les gens doivent réaliser que les attaquants ne ciblent pas exclusivement les appareils eux-mêmes", affirme Alexandru Balan, Responsable des recherches en sécurité chez Bitdefender. "Ils cherchent un point d'entrée facile au sein de votre réseau domestique, qui leur permettra d'accéder à vos autres appareils connectés et de subtiliser toute information non sécurisée circulant au sein du réseau."

À moins que la communication ne soit chiffrée contre l'interception et les altérations, les cybercriminels pourront procéder à une attaque "man-in-the-middle" et dérober les données qui transitent entre l'application, l'appareil et le serveur. S'ils obtiennent l'accès intégral, ils pourront également falsifier l'information, faire planter l'appareil ou l'impliquer dans une attaque DDoS contre des cibles en ligne, à l'insu de l'utilisateur.

Interrogés au sujet de ces potentiels vols de données sur leurs appareils, les Australiens et les Roumains sont les plus inquiets. 42% des Australiens citent cela comme leur préoccupation principale. 39% des Roumains, 37% des Américains, 33% des Britanniques, 30% des Français et 25% des Allemands le citent également.

## *Préoccupations liées au vol de données*




## *Conseils de sécurité afin d'éviter les intrusions*

Afin d'éviter que des personnes malintentionnées parviennent à intercepter leurs communications, les utilisateurs soucieux de leur vie privée se doivent d'améliorer la sécurité de leur réseau en renforçant leurs identifiants, en activant le chiffrement du réseau et en maintenant à jour le firmware de leurs appareils. Une solution de sécurité dédiée à l'IoT[3] est également essentielle pour nettoyer le trafic et bloquer les tentatives d'attaques man-in-the-middle.

2 https://labs.bitdefender.com/2016/11/smart-webcam-can-go-rogue-to-spy-on-kids-bitdefender-finds/
3 http://www.bitdefender.fr/box/

# L'importance des mises à jour

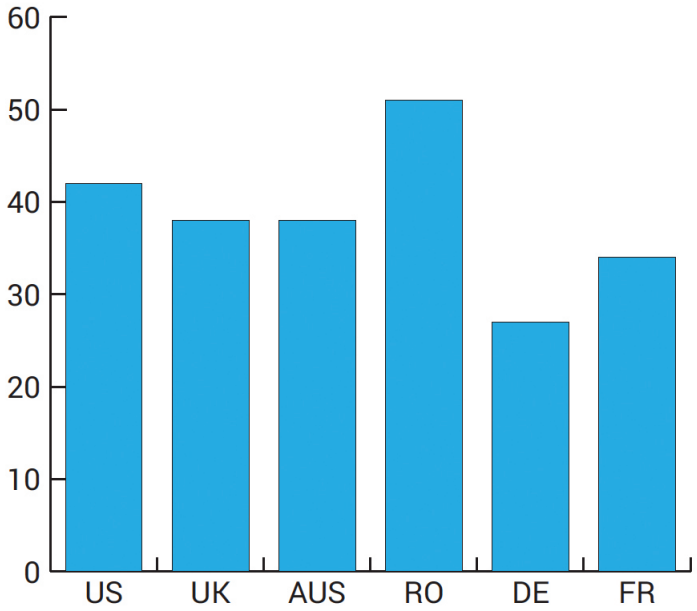
Les télévisions connectées figurent parmi les appareils connectés les plus populaires. En 2017, 244 millions d'unités devraient être vendues à l'échelle mondiale, d'après les statistiques.[4] Bien évidemment, ces télévisions connectées seront équipées de fonctions intégrées capables d'accéder à des services de streaming, d'exécuter des applications et d'aller sur Internet avec des navigateurs.

Aux États-Unis et au Royaume-Uni, 23% des propriétaires de télévisions connectées utilisent leur appareil pour naviguer sur Internet, tout comme 38% des utilisateurs roumains, 26% des utilisateurs australiens, 24% des utilisateurs allemands et 17% des utilisateurs français.

Cependant, **la plupart des utilisateurs ont tendance à négliger les mises à jour.**

42% des Américains n'ont jamais mis à jour leur firmware ou applications. Par rapport à ces mises à jour, la situation semble similaire chez les utilisateurs roumains (51%), britanniques et australiens (38%), allemands (27%) et français (34%).

## *Fréquence des mises à jour de logiciels*



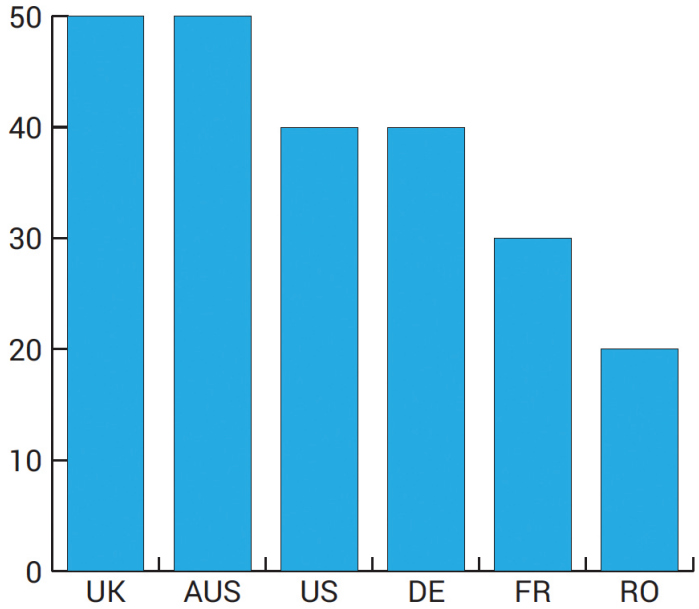

Pour la plupart des utilisateurs, la principale raison invoquée reste le manque de connaissances, comme le confirment 4 utilisateurs américains sur 10, suivie par le manque de temps et la peur d'endommager le système.

Les mises à jour automatiques impliquent généralement peu de clics, quelques minutes et un minimum de compétences techniques, tandis que les mises à jour manuelles requièrent un ordinateur et un périphérique USB. Pour mettre à jour manuellement le firmware de la télévision connectée, l'utilisateur doit se rendre sur la page de téléchargement du fabricant, choisir la dernière version et cliquer pour télécharger le fichier de mise à jour sur un ordinateur. Ensuite, il doit transférer l'exécutable sur une clé USB et l'insérer dans le port USB de la TV.

Le manque d'expertise est invoqué par plus de la moitié des utilisateurs britanniques et des répondants australiens, ainsi que par 4 utilisateurs allemands et américains sur 10, et 2 utilisateurs roumains sur 10. Les 3 utilisateurs français sur 10 n'ayant pas mis à jour le logiciel de leur télévision connectée affirment ne pas avoir eu le temps ou pensent que les mises à jour de logiciel n'ont aucune utilité.

4 www.statista.com/statistics/314616/smart-tv-unit-shipment-worldwide-forecast/forecast/

*Nombre de raisons évoquées pour la non mise à jour de leur TV connectée*




## Conseils de sécurité à l'attention des propriétaires de télévisions connectées

Suite à l'achat d'une télévision connectée, Bitdefender conseille aux usagers de renforcer leur vie privée et de :

- Sécuriser leurs routeurs sans fil avec des mots de passe complexes et uniques.
- Isoler la télévision connectée sur un réseau séparé, dans la mesure du possible.
- N'installer que des applications validées, proposées par le fabricant.
- Utiliser des mots de passe complexes pour chaque compte Internet (Netflix, Facebook, Skype, etc.)
- Si la télévision possède une caméra intégrée, l'éteindre lorsqu'elle n'est pas utilisée.
- Refuser tout message inattendu apparaissant sur votre écran de TV, vous demandant l'autorisation de connecter un appareil ou d'activer une session à distance.
- Utiliser une solution de sécurité dédiée à la protection du foyer permettant de stopper les malwares, les tentatives de phishing et les faux utilisateurs.

# Habitudes de mots de passe

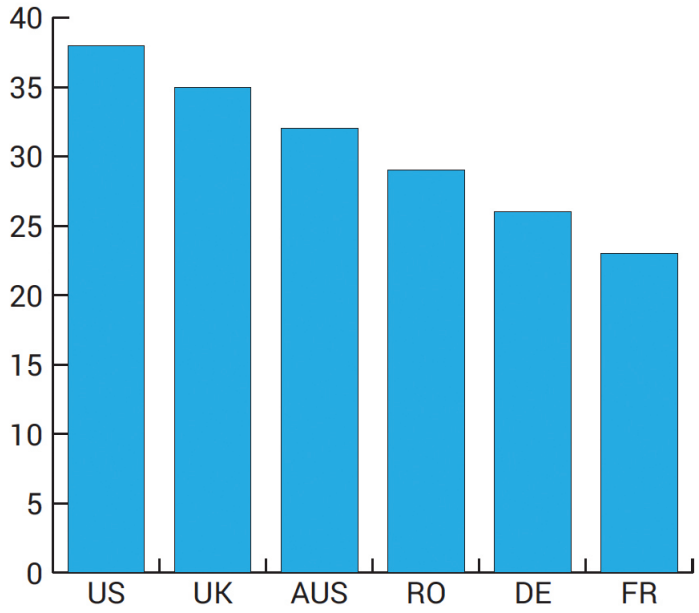
Au Royaume-Uni, en Australie, en Allemagne et en France, 5 propriétaires de télévisions connectées sur 10 ont affirmé ne jamais avoir changé de mot de passe sur leur appareil. De manière identique, 4 utilisateurs roumains et américains sur 10 affirment ne jamais l'avoir modifié.

Les autres appareils sont tout aussi négligés. Par exemple, 4 utilisateurs américains sur 10 affirment ne jamais avoir changé de mot de passe par défaut sur leurs smartphones et tablettes.

Plus inquiétant encore, **16% des utilisateurs américains utilisent le même mot de passe sur l'ensemble de leurs appareils.** Cependant, 45% des utilisateurs américains affirment avoir un mot de passe différent pour chaque appareil. Les utilisateurs français et allemands donnent un meilleur exemple, avec plus de la moitié (57% et 56% respectivement) affirmant disposer d'un mot de passe différent pour chaque appareil, suivis par les utilisateurs britanniques (47%), australiens (46%) et roumains (43%).

Lorsqu'il est question de réutiliser les mots de passe, près d'un tiers des utilisateurs — précisément 38% des Américains, 35% des Britanniques, 29% des Roumains, 23% des Français, 26% des Allemands et 32% des Australiens — affirment avoir plusieurs mots de passe, avec lesquels ils jonglent selon les comptes.

## *Les dangers que présente l'alternance de mots de passe*




La réutilisation du mot de passe est à l'origine de quelques-unes des pires intrusions de sécurité à ce jour. Un pirate est parvenu à infiltrer Dropbox, à cause de la fuite du mot de passe d'un employé, qui s'avérait être le même que celui de son compte Linkedin. Le pirate a ainsi pu accéder au réseau interne de Dropbox, où 68 millions d'identifiants d'utilisateurs étaient stockés.

Malgré ce genre d'exemple, les objets connectés sortent souvent sur le marché sans disposer de mécanismes d'authentification et de sécurisation rigoureux. Des données publiquement divulguées ont révélé que ces appareils ne sont sécurisés qu'avec des mots de passe de type "1234", voire ne disposent d'aucun mot de passe. Par conséquent, les attaques par force brute suffisent bien souvent à craquer les mots de passe et donnent aux pirates la possibilité d'accéder facilement à l'appareil piratés, puis au réseau de l'utilisateur.

"Pratiquement tous les gadgets que nous avons examinés, dans le cadre de notre recherche sur les objets connectés, font état d'une fragilité au niveau des identifiants et d'une absence d'authentification au niveau des hotspot", affirme Alexandru Balan, Responsable des recherches en sécurité chez Bitdefender. "Le fait de changer les mots de passe par défaut est une pratique sécuritaire essentielle, et pourtant, de nombreux utilisateurs l'ignorent toujours."

### *Conseils de sécurité afin de protéger les comptes*

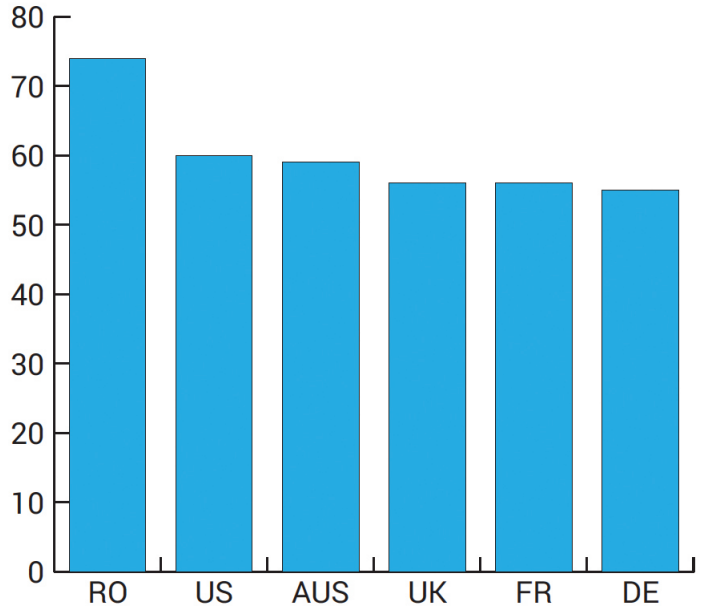
Les utilisateurs ne doivent pas oublier d'attribuer des mots de passe uniques et complexes à leurs comptes et appareils, peu importe si les fabricants le leur rappellent ou non. Dans la mesure du possible, le fait d'appliquer un niveau de protection supplémentaire, par le biais de méthodes d'authentification à deux facteurs, peut également se révéler essentiel pour réduire le risque de piratage de comptes.

## Prévention des pertes de données

Les principaux risques de sécurité qui menacent l'IoT sont liés à la perte d'informations confidentielles, telles que des photos, des documents, des identifiants de comptes, des adresses e-mail, des mots de passe réseaux et des coordonnées bancaires. Les sauvegardes de données sont donc essentielles. Nous avons demandé aux utilisateurs comment ils procédaient pour stocker et sauvegarder leurs données les plus précieuses, et voici ce que nous avons constaté.

Aux États-Unis, 60% des utilisateurs conservent leurs photos et documents confidentiels sur leurs ordinateurs, un chiffre uniquement dépassé par les Roumains, qui atteignent les 74%. Les autres pays affichent des pourcentages similaires : 56% pour les utilisateurs britanniques, 59% pour les Australiens, 56% pour les Français et 55% pour les Allemands.

### *Solutions de sauvegarde les plus prisées*




"Le fait de conserver des données personnelles importantes sur des appareils connectés à Internet augmente les chances de les perdre suite à une infection par des ransomwares, par exemple", explique Balan.

Près de 13 millions de personnes ont été la cible de ransomwares aux États-Unis. Pourtant, 32% des utilisateurs non touchés par les ransomwares pensent qu'il est peu probable, voire très peu probable, qu'ils soient infectés un jour, d'après une étude Bitdefender[5].

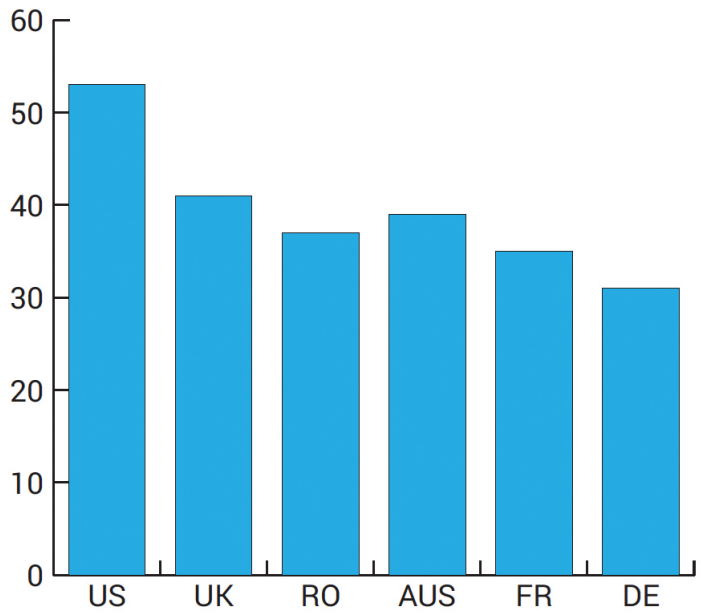
Une des autres solutions de sauvegarde privilégiée est le stockage physique. 47% des utilisateurs américains conservent leurs données personnelles sur des appareils physiques, tels que des périphériques USB ou des DVD. Ce nombre est similaire chez leurs homologues européens — 46% des utilisateurs britanniques, 55% des utilisateurs australiens et 50% des utilisateurs allemands. Les utilisateurs français (62%) en font leur outil de prédilection, et ne sont dépassés que par les Roumains (73%).

Les solutions de stockage dans le cloud apparaissent en deuxième position chez les Américains après les PC personnels : 53% d'entre eux optent pour cette solution, tout comme 41% des utilisateurs britanniques, 37% des utilisateurs roumains, 39% des Australiens, 35% des

5 http://download.bitdefender.com/resources/files/News/CaseStudies/study/59/Bitdefender-Ransomware-A-Victim-Perspective.pdf

Français et 31% des Allemands.

*Niveau de confiance dans le cloud*




Les autres options de stockage comprennent les smartphones, qui se hissent en quatrième position dans cette liste de choix pour la plupart des pays, à l'exception de la Roumaine, où ils apparaissent en 3ème position (42%), et de l'Allemagne ; où ils sont 4ème avec 19% des utilisateurs.

Il est également intéressant de noter qu'aux États-Unis, un tiers des personnes connaissant l'IoT conservent leurs données personnelles sur des ordinateurs portables professionnels, une pratique ayant pourtant des conséquences juridiques, sauf si les règles de la société abordent clairement la question des droits de propriété, de garde et d'accès à ces données.

# Conseils de sécurité afin d'éviter des pertes de données

L'une des pratiques de sauvegarde les plus efficaces consiste à conserver les copies des données précieuses sur un disque dur qui ne soit pas relié à Internet ni au réseau. . Les solutions de stockage dans le cloud sont également des solutions intéressantes, tant que les écosystèmes de cloud sont sécurisés et parviennent à protéger la confidentialité, la disponibilité et l'intégrité des données qui y résident. En 2017, on estime que près de 1,8 milliards de personnes à travers le monde utiliseront un espace de stockage personnel dans le cloud.[6]

6 https://www.statista.com/statistics/499558/worldwide-personal-cloud-storage-users/

# Conclusions

Le concept d'IoT est encore vague pour la plupart des utilisateurs, qui sont plutôt familier avec la notion de “Maison Connectée”. Les principaux risques perçus par les utilisateurs concernent la perte de données personnelles, liée à l'utilisation d'objets connectés mal sécurisés, suivie par l'inaccessibilité de l'appareil et le vol de celui-ci.

En termes de sécurité, les mauvaises habitudes persistent, ou plutôt, le fait de prendre des habitudes plus saines — telles que la mise à jour régulière des logiciels afin de palier aux vulnérabilités ou le fait de changer de mot de passe fréquemment — est toujours aussi dur à mettre en place.

“Même si les fabricants ne répondent pas toujours assez vite avec des mises à jour adaptées aux vulnérabilités découvertes, les utilisateurs ne doivent pas repousser l'installation de celles-ci quand elles sont disponibles” affirme Alexandru Balan, Directeur de la recherche en sécurité chez Bitdefender. “Les cybercriminels infiltrent souvent les réseaux domestiques et professionnels par le biais de logiciels obsolètes : qu'il s'agisse d'un ordinateur portable ou d'un objet connecté, les utilisateurs doivent installer les mises à jour de sécurité avec la même assiduité.”

# Comment améliorer le niveau de sécurité

Avant d'acheter un appareil connecté quel qu'il soit, les utilisateurs devraient essayer d'en comprendre précisément le fonctionnement : comment se connecte-t-il à Internet, à quelles données peut-il accéder, où les données sont-elles stockées et dans quelles conditions ? Une recherche un peu approfondie en ligne sur l'appareil en question permettront aux utilisateurs d'en mesurer les risques et les avantages : ce nouvel appareil présente-t-il une menace en matière de confidentialité ? En utilisant ses données, est-il possible qu'une tierce personne puisse infiltrer le réseau Wi-Fi du domicile pour intercepter des conversations privées ou encore voler des informations personnelles ?

**Lisez la déclaration de confidentialité et toute autre information relative au traitement des données. Les utilisateurs ont tendance à négliger cette étape, pourtant elle peut révéler des faits surprenants. Des informations personnelles peuvent être partagées avec des tiers, tels que des annonceurs, qui sont susceptibles de les utiliser pour créer des campagnes de publicités ciblées et de spammer les utilisateurs.**

**Changez les mots de passe par défaut. Les mots de passe restent le talon d'Achille du domaine de la sécurité, et sont à l'origine des failles de sécurité les plus sévères ayant affecté de grandes sociétés. Par défaut, les appareils sont équipés d'identifiants à la fois simples et faciles à pirater, qu'il est impératif de remplacer par des mots de passe complexes et uniques.**

**Gardez un état précis de l'ensemble de vos appareils domestiques: la manière dont ils fonctionnent, leur niveau de sécurité, qui les utilise chez vous, la publication de mise à jour logicielle par le fabricant et, surtout, si ces appareils sont victimes d'attaques et à quelle fréquence.**

“La gestion des objets connectés au sein d'un foyer est un travail à plein temps qui nécessite beaucoup d'énergie et de nouvelles compétences devant être acquises”, affirme Alexandru Balan . “À mesure que de nouveaux appareils arrivent et constituent le marché existant, nous nous attendons à une montée en compétence en termes de maîtrise de la sécurité des objets connectés.”

Renforcez la sécurité du routeur et utilisez une solution de sécurité dédiée. Si les assaillants parviennent à accéder à un routeur, ils peuvent surveiller, rediriger, bloquer ou falsifier le trafic et les communications sensibles, via ce réseau. En plus de changer les mots de passe, maintenir le firmware à jour et activer le chiffrement WPA2, les utilisateurs devraient renforcer leur sécurité en ajoutant une couche de sécurité supplémentaire.

Bitdefender BOX[7] est la première solution de cybersécurité domestique destinée aux objets connectés. En interceptant les attaques là où elles frappent, c'est-à-dire le réseau domestique, Bitdefender BOX offre une protection avancée contre les malwares avancés et le phishing pour tous les appareils connectés : smartphones, PC, Mac, , technologies portables (wearable),domotique et autres objets connectés. La fonctionnalité d'analyse des vulnérabilités examine les appareils afin de pointer leurs points faibles en terme de sécurité, la fonction Active Threat Control stoppe les malwares inconnus, tandis que la Private Line sécurise toutes les connexions via VPN, même en-dehors du foyer, lorsque vous n'êtes pas connecté au réseau domestique.

Cette étude sur la sécurité de l'IoT a été menée par Bitdefender en août 2016 sur un échantillon de 2037 utilisateurs, originaires de France, des États-Unis, du Royaume-Uni, de Roumanie, d'Australie et d'Allemagne.

7 http://www.bitdefender.fr/box/

**Auteur : Alexandra Gheorghe, Spécialiste en sécurité chez Bitdefender, Novembre 2016**

Bitdefender est une société internationale de technologies de sécurité qui fournit ses solutions dans plus de 100 pays à travers un réseau d'alliances à valeur ajoutée, de distributeurs et de partenaires revendeurs. Depuis 2001, Bitdefender n'a cessé de développer des technologies de protection maintes fois récompensées et est devenu le plus innovant des fournisseurs de technologies de sécurité pour les environnements virtualisés et Cloud. Grâce aux équipes de R&D, d'alliances et de partenariats, Bitdefender a réhaussé les standards de sécurité les plus élevés de l'industrie en s'appuyant à la fois sur ses technologies classées N°1 et ses alliances stratégiques avec les principaux fournisseurs de technologies de virtualisation et de Cloud dans le monde. Plus d'informations sur www.bitdefender.fr



BD-Business-Feb.28.2017-TK#: 70585