DIFFUSION GRAND PUBLIC

CRESITT Industrie
Centre de Ressources Technologiques en Électronique

LAB'O – 1 avenue du Champ de Mars
CS 30019
45074 ORLEANS CEDEX 2

Tél : 02 38 69 82 60 www.cresitt.com

GUIDE CYBERSÉCURITÉ DES IOTs

Version : 1.0

Date : Octobre 2025

Ce projet bénéficie d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre de France 2030. ANR-23-CMAS-0019

SOMMAIRE

1 . INTRODUCTION

1.1 DÉFINITION D'OBJETS CONNECTÉS (IOT) ET DE SYSTÈMES EMBARQUÉS

Les objets connectés (IoT) désignent des dispositifs qui ont la capacité de se connecter à un réseau de communication (Internet des Objets via Wi-Fi, Bluetooth, réseau internet mobile notamment 5G...) et peut selon les cas :

- recevoir, stocker, traiter et transmettre des données,
- recevoir et donner des instructions pour fonctionner.

Ces objets peuvent être autonomes ou fonctionner avec un smartphone ou une tablette permettant de les contrôler ou de servir de relais pour échanger des données.

Ces données peuvent être consultables sur l'appareil mobile ou sur un service Internet.

https://www.economie.gouv.fr/dgccrf/les-fiches-pratiques/objets-connectes-les-risques-connaitre

1.2 IMPORTANCE DE LA CYBERSÉCURITÉ DANS LA VIE QUOTIDIENNE

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 et utilisateurs de ces équipements doivent faire face aux risques des « cybers » attaques.

Une étude de Kaspersky montre que 30 % des entreprises utilisant des systèmes IoT ont subi une attaque majeure en 2022, mettant en évidence des conséquences financières et réputationnelles significatives.

1.3 OBJECTIF DU GUIDE

Ce document vise à sensibiliser le grand public

2 . RISQUES ET MENACES COURANTES

2.1 PRINCIPALES MENACES

Les appareils connectés sont souvent conçus avec des contraintes de coût et de puissance, ce qui peut entraîner des lacunes en matière de sécurité. De nombreux dispositifs manquent de mécanismes de chiffrement et de protection des données, ce qui les rend vulnérables aux attaques :

- De nombreux appareils IoT ne chiffrent pas les données qu'ils envoient, ce qui signifie que toute personne pénétrant dans le réseau peut **intercepter** les identifiants et autres **informations importantes** transmises vers et depuis l'appareil.
- Un autre risque de cette interconnectivité, notamment via internet, est **l'accès non autorisé au réseau** : Même s'il n'y a pas de données importantes stockées sur l'appareil lui-même, un appareil IoT vulnérable peut être une passerelle vers un réseau entier, compromettant ainsi la sécurité de l’ensemble du système.
- Il peut aussi être utilisé comme un « botnet » : les pirates peuvent utiliser sa puissance de traitement pour **distribuer des logiciels malveillants**
- En raison de leur grande quantité et de leur distribution géographique, les dispositifs IoT compromis peuvent être exploités pour inonder un serveur ou une infrastructure avec un trafic malveillant, provoquant ainsi une interruption de service. Ces attaques par « **déni de service** » peuvent perturber gravement les réseaux et les services essentiels.
- Les attaques par **ransomware** sont devenues une menace majeure pour les systèmes IoT. Les pirates informatiques peuvent infiltrer les dispositifs IoT et chiffrer les données, empêchant ainsi leur accès légitime. Ils exigent ensuite le paiement d’une rançon pour débloquer les données.

Sources :

https://www.economie.gouv.fr/dgccrf/les-fiches-pratiques/objets-connectes-les-risques-connaitre

https://www.omogen.com/fr/les-risques-cyber-lies-a-linternet-des-objets-iot-une-menace-grandissante-pour-la-securite-numerique/

https://www.isit.fr/fr/newsletter/iot-risques-enjeux-et-solutions.php

https://www.cyber-cover.fr/cyber-documentation/assurance/linternet-des-objets-connectes-cyber-assurance

2.2 EXEMPLES CONCRETS D'INCIDENTS LIÉS À DES OBJETS CONNECTÉS NON SÉCURISÉS

2.2.1 DOMOTIQUE

- Smart TV (modèle Q60T samsung): Ce modèle fonctionne avec Chromium. En 2021, la version de chromium n'avait pas été totalement mise à jour par Samsung. Le laboratoire Synacktiv s'est servi d'une vulnérabilité non corrigée pour prendre le contrôle de la TV. Une des possibilités ouverte par ce piratage est de pouvoir réaliser des écoutes via cette TV et sa télécommande : https://www.synacktiv.com/sites/default/files/2022-05/Sthack2022_Rooting_Samsung_Q60T_Smart_TV.pdf

- En 2019, une petite fille de 3 ans confie à ses parents qu'une voix lui parle dans le baby-phone vidéo qu'ils ont installé dans sa chambre. Les parents s'aperçoivent que la caméra change toute seule d'orientation. Un pirate, qui avait pris le contrôle à distance de l'objet connecté, les observait et parlait à l'enfant pour l'effrayer quand elle était seule. En 2020, un certain nombre de Babyphones ont été identifiés par la société Safety Detectives comme non sécurisés : le flux vidéo est accessible librement, ce qui veut aussi dire que les images peuvent être vues par des personnes non autorisées, voire malveillantes. Il en est de même pour des caméras de surveillance utilisées dans des magasins, des maisons de retraite ou des garderies pour enfants.

  https://www.safetydetectives.com/blog/babymonitor-exposed-report/

- En 2024, des robots aspirateurs ou tondeuses (notamment de la marque EcoVacs) ont été piratés : certains robots ont eu des comportements anormaux (bruits, poursuite d'animaux domestique, injures, …) mais ils peuvent aussi servir à espionner les propriétaires de façon discrète : Les failles sont nombreuses car ces systèmes sont complexes (connexion au cloud, pilotage par smartphone, mini PC embarqué) et possèdent des capteurs comme des caméras et des microphones qui peuvent être détournés pour de l'espionnage.

  https://www.brut.media/fr/articles/international/etats-unis-canada/des-robots-aspirateurs-pirates-se-sont-mis-a-insulter-leurs-proprietaires

- En février 2025, une plainte a été déposée envers l'assistant vocal Siri d'Apple pour violation de la vie privée. Selon cette plainte, les pratiques d'Apple sont contraires au Règlement général sur la protection des données (RGPD) qui prévoit un consentement "éclairé" des utilisateurs avant toute collecte d'informations personnelles. D'autre part, ces assistants vocaux peuvent être la cible de différentes attaques : soit en passant des commandes sans être entendu des utilisateurs , soit en perturbant le microphone pour que les commandes des utilisateurs ne soient pas prises en compte.

  https://cybersecurite.orange.fr/la-cybersecurite/protection-des-donnees/appareils-sur-ecoute-orange.html

  https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_livre-blanc-assistants-vocaux.pdf (pages 35-36)

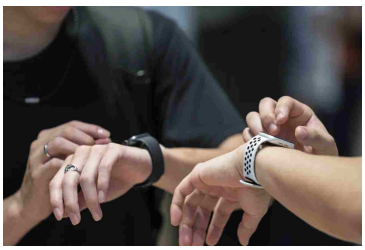
- En 2019, en voulant s'amuser à détourner l'écran tactile d'un robot culinaire vendu par Lidl, deux personnes ont découvert l'existence d'un micro secret inactif, qui pourrait être vulnérable aux attaques.

  https://www.numerama.com/tech/525214-monsieur-cuisine-connect-micro-cache-android-non-securise-les-dessous-du-robot-cuisine-de-lidl.html

2.2.2 SANTÉ

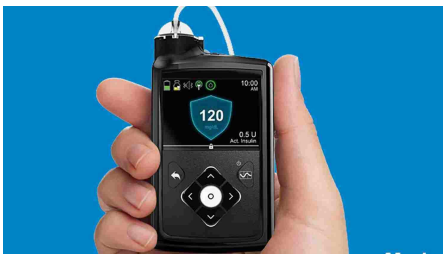
- En 2024 , des chercheurs de Université de Charles Darwin , en Australie, ont pu pirater une variété de montres intelligentes (Smartwatch CF-58 et barcelet Xiaomi) : « Nous pouvions faire baisser ou augmenter la mesure du pouls, voir où une personne est allée et avoir accès à d'autres lectures médicales comme les battements du cœur, la pression artérielle et les relevés de l'ECG. Ces données peuvent être transmises à des sociétés médicales ou être utilisées pour une commercialisation ciblée. »

  Source: https://www.thenewdaily.com.au/finance/consumer/2024/08/25/smart-watches-hackers



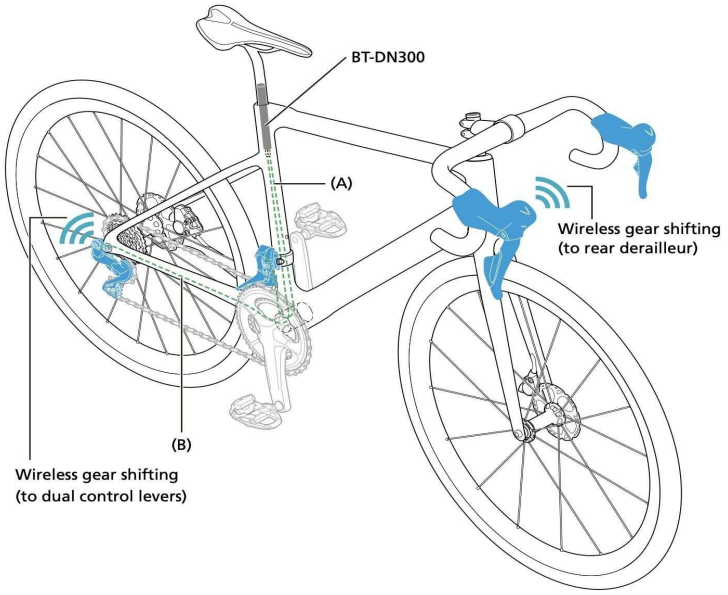
- Entre 2015 et 2020, Marie Elisabeth Gaup Moe, une chercheuse anglaise, a mené des travaux révélant des failles dans les pacemakers Biotronik: Nos recherches ont montré que les références utilisées par l'unité de monitoring à domicile (UMH) pour se connecter à l'infrastructure sont envoyées en clair. En outre, l'UMH n'effectue pas d'authentification mutuelle, ce qui signifie qu'il est possible de s'y connecter à l'aide d'une fausse station de base cellulaire et d'effectuer une attaque de Man-in-the-Middle. Le UMH passe à un canal crypté avant d'envoyer des données de patient, mais les clés de chiffrement sont stockées dans un format récupérable. Cela signifie qu'un attaquant ayant un accès physique à l' UMH peut avoir accès aux identifiants et les utiliser pour l'authentification et le déchiffrement du réseau des données en transit. Cependant, il est impossible de transmettre des commandes aux implants à distance, ce qui évite le potentiel danger de reprogrammer le dispositif du patient et de lui nuire directement. (https://www.mnemonic.io/resources/blog/uncovering-vulnerabilities-in-pacemakers/)

- En 2019, des pompes à insuline de Medtronic ont été rappelées pour faille de sécurité: en raison des vulnérabilités de cybersécurité, un pirate informatique pouvait potentiellement se connecter sans fil à une pompe à insuline Medtronic MiniMed à proximité et modifier les paramètres de la pompe. Dans ce cas, le contrôle des réglages de la pompe pourrait être usurpé au patient, au soignant ou au professionnel de santé et le résultat pourrait être un surdosage ou un arrêt de la distribution d'insuline. https://pmc.ncbi.nlm.nih.gov/articles/PMC6955451/



2.2.3 MOBILITÉ

- En 2024, une équipe de chercheurs de la Northeastern University (Boston) et de l'Université de Californie (San Diego) a analysé la sécurité du système Shimano Di2. Les communications sont en fait assez simples : le levier de vitesse envoie un signal au dérailleur pour qu'il passe à la vitesse supérieure ou inférieure, et le dérailleur confirme la réception de l'ordre. Toutes les commandes sont chiffrées, et la clé de chiffrement semble être unique pour chaque jeu de leviers de vitesse et de dérailleurs. Cependant, les commandes sont toujours les mêmes pour chaque paire de leviers de vitesse/dérailleurs, ce qui rend le système vulnérable à une attaque par rejeu. Cela signifie que les pirates informatiques n'ont même pas besoin de déchiffrer les messages transmis – ils peuvent intercepter les commandes chiffrées et les utiliser pour passer les vitesses sur le vélo d'une victime. https://www.kaspersky.fr/blog/how-to-hack-bicycles-shimano-di2-wireless-shifting-technology/22133/



- En 2024, en déjouant la sécurité du logiciel Tesla, deux experts en sécurité informatique ont réussi à pirater un compte d'utilisateur pour accéder à son véhicule: ils ont créé un faux point d'accès WiFi pour tromper les clients de la marque, mettant en lumière la vulnérabilité des systèmes Tesla face au hameçonnage. https://www.ouest-france.fr/high-tech/deux-ingenieurs-parviennent-a-pirater-une-tesla-pour-en-prendre-le-controle-a-distance-fd218834-dfb8-11ee-9f83-f8f0203f0431

- Les techniques de vol de véhicules sont variées selon le niveau de ces experts du vol 2.0. L'une d'elles consiste à acquérir un kit de piratage négocié, sous le manteau, autour de 5.000 €. « Il s'agit d'une enceinte Bluetooth portative trafiquée dotée d'un câble USB. Le voleur pénètre dans la voiture, puis il se connecte rapidement au tableau de bord pour la démarrer ». Une autre combine des malfrats a été baptisée "CAN injection" [le bus CAN est un bus servant à transporter les données entre différents systèmes numériques de la voiture] :Une faille dans l'avant de la voiture

permet au voleur de relier son boîtier frauduleux à un faisceau de la voiture. Reste à lui envoyer de fausses consignes électroniques pour ouvrir les portières et, surtout, faire démarrer le véhicule. » De nombreuses Toyota Rav 4 et même des Toyota Land Cruiser ont été subtilisées grâce à cette méthode.

https://www.lechorepublicain.fr/chartres-28000/actualites/les-toyota-rav-4-l-une-des-voitures-les-plus-volees-en-france-ciblee-en-eure-et-loir_14312213/

2.2.4 AU TRAVAIL / EN TÉLÉTRAVAIL

- Cyberattaque 1 : l'accès aux dossiers partagés : À votre domicile, vous avez très certainement, et comme la majorité des gens, cliqué sur réseau « privé » ou « domestique ». Or, cette action incite Windows à diminuer sa vigilance et à faire confiance aux autres membres de votre réseau. Il les autorise notamment à découvrir vos éventuels dossiers partagés. Un cyberattaquant ayant accès à votre réseau local peut alors facilement lister vos partages réseaux, y accéder et récupérer tous les documents confidentiels qu'ils contiennent. Selon la configuration de votre partage, il peut même modifier les documents présents ou en ajouter de nouveaux. Comme, par exemple, dissimuler à la place d'un de vos fichiers un RAT (Remote Access Trojan) qui se déclenchera la prochaine fois que vous cliquerez sur ledit fichier pour l'ouvrir. Dans le pire des cas , l'attaquant peut prendre le contrôle de votre ordinateur.
- Cyberattaque 2 : l'exploitation d'une vulnérabilité RCE, par exemple, la CVE-2020-0796, aussi appelée « SMBGhost » permet à un attaquant présent sur votre réseau local d'exécuter du code à distance sur votre machine en exploitant le protocole de partage réseau SMBv3. Ce genre de vulnérabilité est généralement vite patché et rarement communiqué avant la publication de la mise à jour de sécurité corrective. Son exploitation est donc peu probable si votre ordinateur est parfaitement à jour. Cependant, il est fréquent que les ordinateurs professionnels utilisés en télétravail se mettent à jour uniquement lorsqu'ils sont connectés au réseau de l'entreprise.
- Cyberattaque 3 : l'exploitation de la fonction LLMNR : Cette dernière menace, plus technique, consiste à piéger votre ordinateur, afin qu'il révèle vos identifiants à l'attaquant. Comme nous l'avons vu avec le premier risque d'attaque, en se connectant à un « réseau domestique », votre

ordinateur tente de repérer automatiquement tous les services présents sur le réseau. Pour cela, Windows utilise plusieurs protocoles, notamment LLMNR et NBT-NS, afin d'envoyer des requêtes de découverte. Votre ordinateur tente ensuite de contacter les différents services détectés. Si ces derniers requièrent une authentification, votre ordinateur s'y connecte automatiquement avec votre compte utilisateur. Un attaquant présent sur votre réseau peut exploiter ce mécanisme en répondant aux requêtes de découverte et en annonçant des services fictifs demandant une authentification. Dans le pire des cas (anciennes versions de Windows et/ou mauvaises configurations), le pirate peut directement récupérer votre mot de passe. La plupart du temps, il obtient plutôt un code hash permettant de casser votre mot de passe. Plus le mot de passe est faible (court, présent dans un dictionnaire de mots de passe…), plus son cassage est aisé. En récupérant le mot de passe de votre compte Windows, l'attaquant peut ensuite se connecter à tous les services en ligne de votre entreprise dont l'authentification est basée uniquement (sans authentification multifacteur) sur ce compte ou encore utiliser votre mot de passe dans le cadre d'une attaque plus complexe depuis l'intérieur du réseau de votre entreprise.

https://www.alter-solutions.fr/blog/télétravail-3-cyberattaques

- Début février 2024, AnyDesk a fait face à une cyberattaque sophistiquée. Les certificats ont été compromis et un certain nombre d'identifiants sont en vente sur le dark Web. La réaction de l'entreprise inclut la réinitialisation forcée des mots de passe sur le portail client « my.anydesk.com », le changement des certificats pour bloquer les connexions frauduleuses, ainsi qu'une mise à jour de sécurité cruciale. L'entreprise précise que le code source de l'application est sain et qu'il n'a pas été altéré par les pirates pour distribuer un logiciel malveillant.

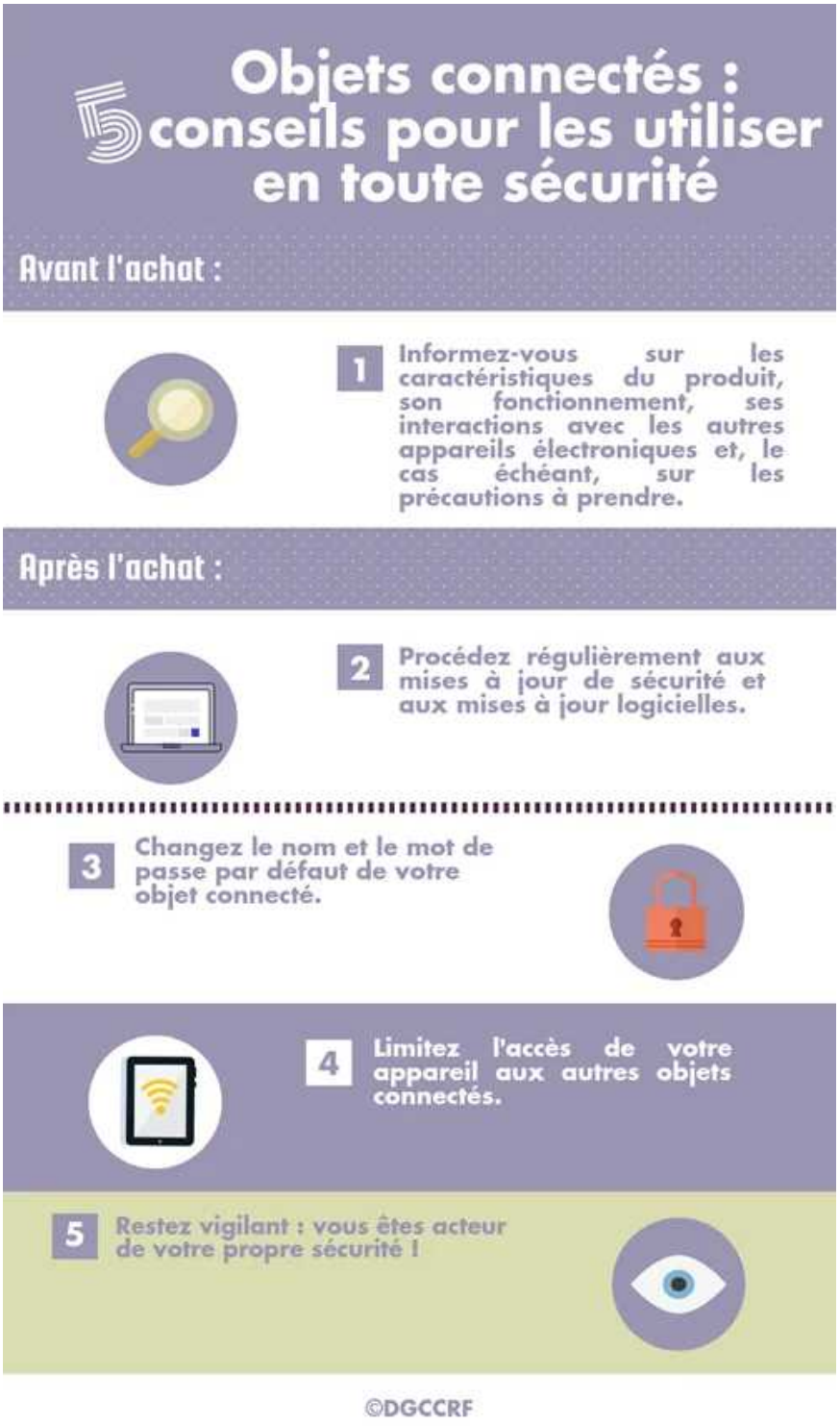
  https://www.carlidev.fr/securite-informatique-piratage-anydesk-2024/

3 . BONNES PRATIQUES

3.1 SÉCURISER SON IOT

On trouve sur internet de nombreuses indications pour la sécurité des objets connectés pour le grand public. Par exemple, les sites https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-objets-connectes-iot et https://www.economie.gouv.fr/dgccrf/les-fiches-pratiques/objets-connectes-les-risques-connaitre sont notamment assez complets.

Voici donc quelques bonnes pratiques à adopter :



Loin d'être toujours assurée, la protection des objets connectés contre le piratage informatique reste un domaine complexe qu'il est difficile d'appréhender. Les solutions complémentaires énoncées ci-dessous ne sauraient garantir l'absence d'attaques mais constituent les mesures de base qui sauront renforcer la sécurité de vos équipements.

3.1.1 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.

Si possible, choisissez des appareils avec des garanties de sécurité reconnues

3.1.2 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 deviner ou publiquement connus, ils n'assurent pas un niveau de sécurité suffisant. Il est donc indispensable de changer le mot de passe par défaut dès la première utilisation et d'utiliser un mot de passe suffisamment long et complexe pour sécuriser votre objet connecté. Il est également conseillé de choisir un mot de passe unique pour chaque appareil.

De façon générale, configurez correctement les paramètres de sécurité dès l'installation et désactivez les fonctionnalités non utilisées pour réduire les risques.

Ces conseils sont également applicables à l'ensemble des appareils de votre réseau numérique.

3.1.3 METTEZ À JOUR SANS TARDER VOS OBJETS CONNECTÉS ET LES APPLICATIONS ASSOCIÉES

Réalisez les mises à jour de sécurité de vos objets connectés et des applications qui peuvent leur être associées dès qu'elles sont disponibles pour éviter que des cybercriminels utilisent des failles de sécurité pour prendre le contrôle de l'objet ou vous dérober des informations personnelles sensibles. Si cela est possible, configurez votre objet connecté pour que les mises à jour se téléchargent et s'installent automatiquement.

3.1.4 PROTÉGEZ VOS INFORMATIONS PERSONNELLES

Pour protéger votre identité numérique et si votre objet connecté nécessite la création d'un compte en ligne, protégez-le par un mot de passe solide et différent de vos autres comptes. Ne communiquez que le minimum d'informations nécessaires (date de naissance aléatoire, âge approximatif, etc.). Utilisez le plus souvent des pseudonymes au lieu de vos noms et prénoms. Créez-vous, si possible, une adresse de messagerie (mail) spécifique pour vos objets connectés afin d'éviter de voir polluée votre adresse principale par des messages indésirables.

3.1.5 VÉRIFIEZ LES PARAMÈTRES DE SÉCURITÉ DE VOS OBJETS CONNECTÉS ET DE LEURS APPLICATIONS

Vérifiez que l'objet ne permet pas à d'autres personnes de s'y connecter en vous assurant que la connexion avec un autre appareil (téléphone mobile, tablette, ordinateur, etc.) ou sur Internet ne peut se faire qu'au travers d'un bouton d'accès sur l'objet ou par l'utilisation d'un mot de passe. Par ailleurs, désactivez les fonctionnalités comme le partage des données sur les réseaux sociaux par exemple, si vous ne l'utilisez pas ou n'en avez pas besoin, pour réduire les risques de piratage et de fuite incontrôlée de vos données personnelles.

3.1.6 ÉTEIGNEZ SYSTÉMATIQUEMENT VOS OBJETS CONNECTÉS LORSQUE VOUS NE LES UTILISEZ PAS

Lorsque vos objets connectés ne sont pas ou plus en cours d'utilisation, pensez à les éteindre ou à les déconnecter pour réduire les risques de piratage, de vol de données ou d'intrusion malveillante.

3.1.7 METTEZ À JOUR LES APPAREILS RACCORDÉS À VOS OBJETS CONNECTÉS

Si vos objets connectés sont associés à d'autres appareils (téléphone mobile, tablette, ordinateur, etc.), effectuez également leurs mises à jour sans tarder pour éviter que des cybercriminels puissent accéder à ces appareils en utilisant une faille de sécurité et ainsi atteindre vos objets connectés. N'oubliez pas de mettre également à jour votre « box » Internet en la redémarrant régulièrement car c'est généralement par ce biais que vos objets se connectent à Internet.

3.1.8 SÉCURISEZ VOTRE CONNEXION WI-FI

Si vos objets connectés envoient ou reçoivent des informations par le biais de votre connexion Wi-Fi, il est essentiel de la sécuriser pour réduire les risques de piratage et de prise de contrôle à distance de vos objets. Pour cela utilisez un mot de passe solide et vérifiez que votre connexion utilise le chiffrement en « WPA2 » qui est aujourd'hui la méthode de chiffrement Wi-Fi la plus sûre.

3.1.9 LIMITEZ L'ACCÈS DE VOS OBJETS CONNECTÉS AUX AUTRES APPAREILS ÉLECTRONIQUES OU INFORMATIQUES

Pour limiter les risques de piratage, n'autorisez l'association (ou « appairage ») de vos objets connectés qu'aux seuls appareils nécessaires aux fonctionnalités dont vous avez besoin. Par exemple, la poupée connectée de votre enfant n'a pas forcément besoin de dialoguer avec votre réfrigérateur connecté. Si vous en avez la possibilité, il est également recommandé d'utiliser ses objets connectés sur un réseau distinct (réseau privé virtuel ou VLAN) des autres équipements informatiques de votre environnement.

3.1.10 SUPPRIMEZ VOS DONNÉES ET RÉINITIALISEZ VOTRE OBJET LORSQUE VOUS NE VOUS EN SERVEZ PLUS

Si vous êtes amené à vous séparer de votre objet connecté (vente, panne…), et afin d'éviter que l'on puisse accéder à vos informations personnelles qu'ils peuvent contenir, effacez vos données sur l'objet connecté et supprimez le compte en ligne auquel il peut être associé. Si l'objet est associé à vos différents comptes en ligne comme vos comptes de réseaux sociaux, supprimez également cette association. Par ailleurs, réinitialisez l'objet dans ses paramètres par défaut (configuration usine) si cela est possible pour réduire les risques d'accès à des données personnelles qu'il pourrait contenir comme par exemple votre mot de passe Wi-Fi.

→ Vous êtes acteurs de votre sécurité !

3.2 PROTÉGER SES DONNÉES PERSONNELLES

Pour se prémunir des cyberattaques, la CNIL (Commission nationale de l'informatique et des libertés), dont la mission est de protéger le consommateur contre toute utilisation abusive de données informatiques, recommande d'adopter certains gestes simples mais efficaces :

- vérifier que l'objet ne permet pas à n'importe qui de s'y connecter sans utiliser un mot de passe ou un bouton d'accès physique. Les objets fonctionnant *via* la fonction Bluetooth sont plus facilement piratables ;
- changer le paramétrage par défaut de l'objet (mot de passe, code PIN, etc.) ;
- sécuriser le réseau WIFI à l'aide d'un mot de passe ;
- désactiver le partage automatique des données ;
- s'assurer de la possibilité d'accéder aux données et de pouvoir les supprimer ;
- effectuer régulièrement les mises à jour des logiciels ;
- éteindre l'objet quand il n'est pas utilisé.

Dans le cas où l'utilisation d'un objet connecté nécessite la création d'un compte en ligne, la CNIL recommande également de veiller à anonymiser le plus possible les données : Il s'agira alors de recourir aux pseudonymes, de créer une adresse de messagerie dédiée aux objets connectés ou encore de communiquer le minimum d'informations personnelles lors de leur activation.

Par ailleurs, au moment de s'équiper en objets connectés, il est préférable d'orienter son choix vers des marques qui font référence sur le marché, ces dernières proposant souvent des produits mieux sécurisés que ceux distribués par des marques moins reconnues. Enfin, avant tout achat, il est vivement conseillé de demander l'avis d'un professionnel qui sera en mesure de vous aiguiller pour choisir le produit qui répondra le mieux à vos besoins.

(source https://www.promotelec.com/particuliers/fiche/comment-utiliser-un-objet-connecte-sans-se-faire-pirater/#quelques-solutions-a-appliquer)

3.3 SÉCURISATION DES COMMUNICATIONS SANS FIL

3.3.1 CONSEILS POUR SÉCURISER VOTRE RÉSEAU WI-FI DOMESTIQUE

- Changez le mot de passe par défaut, avec un mot de passe robuste
- Définissez un mot de passe unique pour votre compte administrateur WiFi et routeur : Ne laissez pas votre routeur fonctionner avec les mots de passe WiFi et administrateur par défaut. Les pirates tentent constamment de s'introduire dans des appareils en utilisant ces informations d'identification publiquement connues. C'est aussi une bonne habitude de changer régulièrement le mot de passe.
- Activez le chiffrement WPA3 qui est beaucoup plus robuste aux attaques que le WPA2 : les mots de passe échangés à la connexion sont beaucoup plus difficiles à intercepter et la clé de chiffrement comporte 256 bits à la place de 128 sur les versions antérieures.
- Gardez le firmware à jour : Des correctifs de sécurité et des corrections de bugs sont insérés dans les derniers firmwares pour réparer les vulnérabilités réseau récemment exposées. Un routeur avec des mises à jour automatiques est la meilleure option, mais vous devrez vous assurer que vous les avez activées.
- Créez un réseau d'invités : Sans refuser l'accès WiFi à vos invités, mais sans compromettre la sécurité de votre réseau, il peut être possible de configurer un réseau invité, si votre routeur WiFi prend en charge cette fonction. Un réseau invité est isolé du réseau domestique, les visiteurs auront accès à Internet sans avoir le potentiel d'accéder à vos données privées.
- Vous pouvez également ajouter une liste blanche d'appareils autorisés à accéder à votre réseau
- Désactivez les fonctions WPS et UpnP : Certains routeurs WiFi ont un bouton de couplage ou un bouton WPS pour faciliter la connexion car vous n'aurez pas à entrer le mot de passe pour ajouter de nouveaux appareils à votre réseau. Cependant, bien que cela soit pratique, il peut également être exploité pour accéder à votre réseau domestique. De même, UPnP (Universal Plug and Play) est conçu pour faciliter la connexion d'appareils tels que les téléviseurs intelligents sans configuration complexe. Mais certains programmes malveillants ciblent UPnP pour accéder à votre réseau domestique. Si la sécurité du réseau est une préoccupation majeure pour vous, il est plus sûr de désactiver ces fonctions.

Sources : https://www.okta.com/fr/identity-101/wpa3-security/ , https://www.tp-link.com/fr/support/faq/2970/

3.3.2 RISQUES LIÉS AUX CONNEXIONS À DES RÉSEAUX WI-FI « GRATUITS »

Les réseaux Wi-Fi publics des restaurants, des hôtels, des magasins ou des aéroports nous permettent de connecter notre ordinateur ou notre smartphone partout, la plupart du temps sans débourser un centime. Mais on oublie souvent que nous nous exposons alors à de nombreux dangers en ligne :

- Contrairement aux réseaux Wi-Fi privés que vous utilisez chez vous ou au travail, les réseaux ouverts ne comportent généralement pas d'éléments de protection tels que des mots de passe. Ainsi, n'importe qui peut s'y connecter de manière pratiquement anonyme. Ce manque de sécurité, associé à la grande créativité des cybercriminels, a multiplié le nombre d'arnaques en ligne. Voici une liste des escroqueries les plus courantes :

- Les faux réseaux Wi-Fi : c'est l'un des outils les plus utilisés par les pirates pour obtenir des informations sensibles. La technique consiste à créer un réseau Wi-Fi avec le nom de l'établissement où le signal est reçu, comme un bar ou un restaurant, afin d'accéder à l'appareil de la victime.
- L'attaque « man in the middle »: avec ce type de cyberattaque, le pirate parvient à intercepter la transmission des données entre la victime et le site web qu'elle visite. Cela lui permet d'accéder à une grande quantité d'informations avec un faible risque de détection.
- Les logiciels malveillants (malware) : grâce à l'anonymat offert par les réseaux Wi-Fi ouverts, les pirates peuvent accéder aux smartphones et aux ordinateurs portables et les infecter avec des logiciels malveillants pour les endommager ou voler des informations sensibles.
- Le logiciel ramsonware : les cybercriminels font du chantage auprès de leurs victimes. Ils bloquent des fonctions de son ordinateur, comme le clavier ou la souris, ou cryptent des fichiers importants (images, informations bancaires ou documents importants) puis réclament de l'argent pour reprendre le contrôle de l'ordinateur.
- Le vol de données : l'un des risques les plus courants lors de la connexion à un réseau Wi-Fi public est le vol des informations contenues dans les fichiers de notre appareil. Des données personnelles, professionnelles ou des mots de passe peuvent alors finir par tomber entre de mauvaises mains.

3.3.3 SE PROTÉGER SUR UN RÉSEAU WI-FI PUBLIC

- Vérifier les noms des réseaux : méfiez-vous des noms de Wi-Fi douteux qui vous redirigent vers des pages qui vous demandent beaucoup d'informations pour vous connecter. Assurez-vous aussi qu'il s'agit bien du réseau de l'établissement où vous vous trouvez.
- Avoir un antivirus à jour : Vous avez probablement déjà un antivirus sur votre ordinateur, mais assurez-vous que le pare-feu de votre appareil est activé. Cela peut aider à bloquer les tentatives d'intrusion et à renforcer la sécurité globale de votre connexion. Il est aussi conseillé d'installer un anti-virus sur votre téléphone mobile, surtout si vous l'utilisez pour vous connecter à des réseaux Wi-Fi publics. Il existe plusieurs antivirus gratuits pour iPhone et Android qui détectent la présence de logiciels malveillants sur votre mobile.
- Installer un VPN : les applications de réseau privé virtuel ou VPN servent principalement à simuler que vous vous connectez à Internet à partir d'un autre réseau. Cela rend donc la tâche beaucoup plus difficile pour les cybercriminels potentiels qui souhaitent accéder à votre appareil. La plupart de ces applications sont gratuites, alors n'hésitez pas à les utiliser.
- Désactiver le partage de fichiers : Il est recommandé de désactiver les paramètres de partage de fichiers sur vos appareils si vous vous connectez aux réseaux Wi-Fi publics. Ceux connectés à ce même réseau pourraient accéder à vos données locales.
- Effectuer les mises à jour : la plupart des mises à jour logicielles pour smartphones, tablettes et ordinateurs portables incluent des améliorations de la protection des appareils. Si vous maintenez à jour les appareils avec lesquels vous vous connectez aux réseaux Wi-Fi publics, vous pourrez surfer sur internet avec une plus grande sécurité.
- Ne vous connectez pas à des applications sensibles depuis un réseau Wi-Fi ouvert : par exemple ne

vous connectez pas à votre banque en ligne ou votre messagerie, ne faites pas d'achats en ligne. En effet, il sera beaucoup plus facile pour les pirates d'obtenir des informations sensibles comme vos transactions ou le mot de passe de vos comptes. Si vous devez le faire, assurez-vous que le site est sécurisé (URL commençant par « https:// ») et utilisez un VPN.

Sources : https://n26.com/fr-fr/blog/risques-wifi-public , https://cerfrance22.fr/2024/02/28/wi-fi-publics-risques-et-bonnes-pratiques/

3.4 CONSEILS SPÉCIFIQUES

3.4.1 POUR LES ASSISTANTS VOCAUX

1. Désactiver l'activation automatique et utiliser un bouton physique si possible.
2. Vérifier les paramètres de confidentialité et limiter la conservation des enregistrements vocaux

Sources : https://cybersecurite.orange.fr/la-cybersecurite/protection-des-donnees/appareils-sur-ecoute-orange.html, https://www.cnil.fr/fr/les-conseils-pour-configurer-et-utiliser-son-assistant-vocal

3.4.2 POUR LES BABYPHONES, CAMÉRAS DE SURVEILLANCE OU INTERPHONES VIDEO :

Il faut se poser deux questions : avez-vous besoin d'un mot de passe ou de vous authentifier à chaque consultation de la vidéo et avez-vous dû créer un mot de passe personnalisé lors de votre première connexion ? Si les deux réponses sont négatives, le flux vidéo du babyphone ou de la caméra est probablement en accès libre sur Internet…

Source : https://www.leparisien.fr/high-tech/des-failles-de-securite-decouvertes-dans-des-babyphones-16-02-2021-2KQA5WZPMVAZXP235BXNY4F7YY.php

3.4.3 POUR LES DISPOSITIFS MÉDICAUX

- Lorsque vous achetez ou obtenez un dispositif médical, vous devez comprendre les risques de cybersécurité. Selon la question, votre médecin ou le fabricant de l'appareil médical peut vous aider. En ce qui concerne la cybersécurité, les questions à se poser pourraient notamment être les suivantes:
  - Quels sont les risques pour la cybersécurité associés à l'utilisation de mon appareil?
  - Quels sont les paramètres de sécurité par défaut?
  - Qu'advient-il de la sécurité de l'appareil si je change les paramètres par défaut ?
  - Quand et comment cet appareil se connecte-t-il à Internet ? Y compris le WiFi à domicile, les réseaux mobiles et le WiFi public.
  - Qui a accès aux informations sur mon appareil ou mon smartphone ? Où va-t-elle ?

- Comment puis-je savoir si un appareil a été piraté ou compromis et à qui devrais-je m'en parler si cela est suspecté?
- Que dois-je faire pour maintenir l'appareil (mise à jour)?
- Dois-je vérifier les paramètres du smartphone ? Par exemple, les paramètres des mots de passe et les paramètres de connectivité.

- Éteindre les fonctions que vous n'utilisez pas : Votre appareil peut avoir des capacités de communication que vous n'utilisez pas ou dont vous n'avez pas toujours besoin. Un exemple est une capacité Bluetooth qui permet automatiquement à votre appareil de se connecter à votre ordinateur ou à un réseau WiFi proche. Si vous n'utilisez pas cette fonction ou si vous ne l'utilisez pas parfois, vous devez éteindre la fonction lorsque cela n'est pas nécessaire. Vous devez en parler à votre médecin avant d'éteindre tout dispositif.

  Source: https://www.tga.gov.au/safety/safety/medical-device-cyber-security-consumer-information

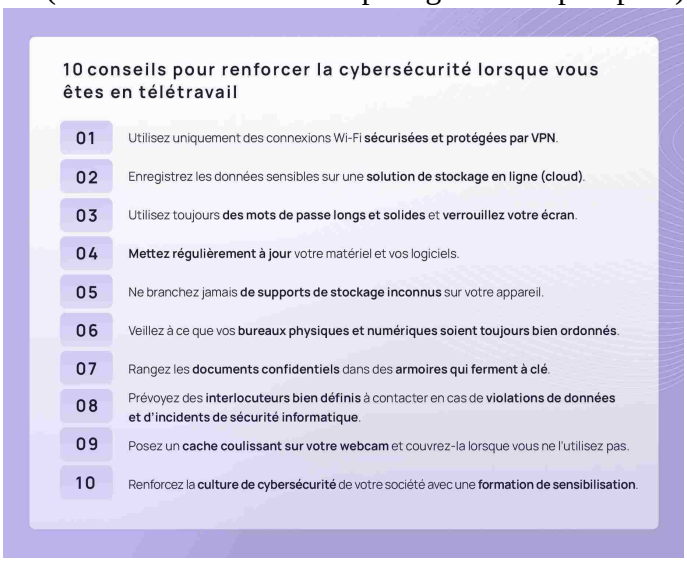
3.4.4 POUR LES VÉHICULES :

- Clés sans contact :
  - utiliser une pochette de protection anti-RFID qui bloque les ondes radio lorsque la clé n’est pas utilisée.
  - désactiver la fonction sans contact lorsque cela est possible
  - conserver la clé à distance des portes et fenêtres afin de limiter les risques d’interception du signal.
- De nombreux véhicules récents permettent d’effectuer des mises à jour à distance (OTA – Over-The-Air). Si votre voiture dispose de cette option, assurez-vous qu’elle est activée et configurée pour recevoir automatiquement les correctifs de sécurité. Pour les modèles plus anciens nécessitant une mise à jour manuelle, il est recommandé de vérifier régulièrement auprès du fabricant ou du concessionnaire.

  Source : https://iodines.fr/comment-empecher-les-hackers-de-prendre-le-controle-de-votre-vehicule/

3.4.5 EN TÉLÉTRAVAIL :

- 10 règles en télétravail (valable aussi en bureau partagé ou en openspace) :



https://sosafe-awareness.com/fr/blog/10-conseils-pour-teletravailler-en-toute-securite/

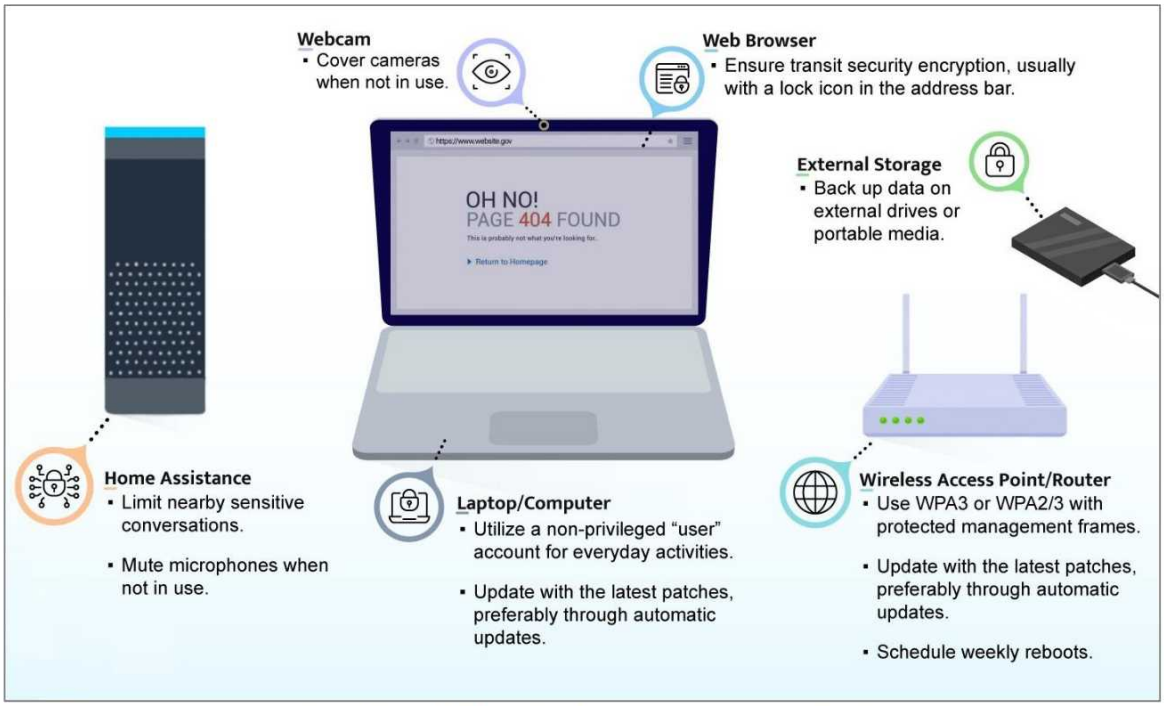


Figure: Several best practices for securing your home network

https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF

- Prévention et Protection contre le Piratage d'Imprimantes (https://labo.toner.fr/le-saviez-vous/piratage-dimprimante-comment-sen-proteger/ et https://axidoc.com/cybersecurite-les-scanners-et-imprimantes-sont-ils-vulnerables)
  - Limiter l'accès physique aux MFP afin de restreindre les manipulations non autorisées

- Mettre en place un système de surveillance et de traçage de l’utilisation des systèmes d’impression
- Protégez votre réseau : Assurez-vous que votre réseau WiFi ou Bluetooth est sécurisé par un mot de passe robuste.
- Configurer un mot de passe d'administration : Limitez l'accès non autorisé en mettant en place un mot de passe d'administration pour votre imprimante.
- Utilisez un chiffrement solide : Améliorez la sécurité de votre réseau sans fil en optant pour le chiffrement WPA2 ou WPA3.
- Soyez vigilant avec les clés USB : Les pirates peuvent utiliser des clés USB infectées pour compromettre l'imprimante et le réseau. Désactivez les ports USB lorsque vous n'en avez pas besoin et vérifiez les clés USB avant de les utiliser.
- Masquez le nom de votre réseau : Rendez votre réseau invisible aux scanners malveillants et activez la détection d'intrusion pour être alerté en cas de tentative d'accès non autorisé.

- Lorsque votre ordinateur se connecte à un réseau, ne le déclarez jamais en réseau « privé » à moins que vous ayez une confiance absolue en tous les équipements qui y sont connectés.
- Ne partagez jamais de fichier ou de dossier sensible à tout le monde.
- Ne donnez jamais le droit d’écriture à tous sur un de vos fichiers ou dossiers partagés.

4 . QUE FAIRE EN CAS DE PROBLÈME ?

Voici quelques pistes pour savoir si votre appareil pourrait être compromis:

- la batterie se vide plus rapidement que d'habitude
- vous constatez des pics d'utilisation des données Internet alors que vos habitudes n'ont pas changé. Des outils tels que des moniteurs de réseau ou des routeurs avec des analyses intégrées peuvent être précieux pour identifier ces pics.
- Un comportement inattendu du dispositif : Le système peut s'allumer ou s'éteindre sans action de l'utilisateur, modifier spontanément les paramètres ou effectuer des tâches en dehors de sa fonction normale. Il peut aussi ne pas tenir compte des commandes envoyées par l'utilisateur.
    - Par exemple, une ampoule intelligente peut commencer à clignoter de manière erratique, ou une caméra de sécurité peut s'activer sans commande. Ces anomalies indiquent souvent un accès non autorisé.
    - Pour les smartphones, vous ou vos contacts recevez des appels ou des messages étranges, des pop-ups publicitaires aléatoires ou des applications inconnues sont installées sans votre autorisation , des applications qui fonctionnaient bien auparavant commencent à avoir un comportement étrange, l'historique de vos appels et de vos messages texte comporte des entrées étranges.

Quelques conseils à suivre en cas de compromission de vos appareils :

1. Déconnecter le dispositif: Isolez le système compromis du réseau pour éviter d'autres dommages ou d'exfiltration de données.
2. Mise à jour du logiciel: Veiller à ce que les derniers correctifs de sécurité et les mises à jour du logiciel soient appliqués.
3. Réinitialiser le système: Effectuez une réinitialisation d'usine pour supprimer tout logiciel malveillant. Reconfigurer l'outil avec des mots de passe et des paramètres de sécurité forts et uniques. Pour un téléphone, vous pouvez identifier l'application responsable de comportements étranges en ouvrant le menu des applications récentes et en appuyant longuement sur l'icône de l'application. Ensuite vous pouvez désinstaller cette application
4. Surveiller le trafic réseau: utiliser des outils de surveillance du réseau pour identifier et analyser le trafic suspect. La surveillance de l'activité du réseau peut aider à détecter les activités malveillantes.
5. Consulter les professionnels de la sécurité: si la situation semble complexe ou au-delà de l'expertise personnelle, consulter les professionnels de la cybersécurité qui pourront fournir une analyse plus approfondie et des correctifs.

Sources : https://www.welivesecurity.com/fr/2022/02/02/signes-telephone-pirate/
https://www.iotforall.com/indicators-of-compromise-12-signs-your-iot-device-was-hacked

Ressources et contacts utiles pour obtenir de l'aide : www.cybermalveillance.gouv.fr . Sur ce site, un questionnaire de diagnostic est aussi disponible : https://www.cybermalveillance.gouv.fr/diagnostic

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/cyberattaque-consignes-collaborateurs

5 . QUE DIT LA LOI ?

Pour la protection des données privées, le Règlement Général sur la Protection des Données (RGPD) en Europe impose des exigences strictes pour la protection des données personnelles, affectant également les dispositifs IoT. Les entreprises doivent s'assurer que les dispositifs collectant des données personnelles sont sécurisés et que les données sont traitées conformément aux principes du RGPD. Cela inclut des mesures telles que l'anonymisation des données, la minimisation des données collectées et le consentement explicite des utilisateurs.

Depuis le 1er janvier 2022, le vendeur d'un bien comportant des éléments numériques, doit informer les consommateurs de la durée durant laquelle les mises à jour logicielles que le producteur fournit, restent compatibles avec les fonctionnalités du bien (source https://www.economie.gouv.fr/dgccrf/les-fiches-pratiques/objets-connectes-les-risques-connaitre , https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044125847, article 3)

La directive pour les équipements radio (RED) existe depuis 2020. Depuis janvier 2025, la Commission européenne a intégré une norme (norme EN 18031 « Exigences de sécurité commune pour les équipements radio ») pour faire en sorte que tous les équipements communicant sans fils soient conformes aux prescriptions en matière de cybersécurité énoncées dans les articles de la directive, à savoir :

- Assurer que les équipements radio communiquant sur Internet ne peuvent pas compromettre ou nuire aux réseaux
- Garantir la sécurité des données à caractère personnel et de la protection de la vie privée dans les équipements radio
- Protèger les utilisateurs contre la fraude lorsqu'ils utilisent des équipements hertziens pour des transactions financières

Ces exigences s'appliquent aux appareils qui intègrent la technologie radio et se connectent à Internet. Elles seront applicables en août 2025.

Source : https://acepelec.com/norme_europeennee_en_18031_pour_la_cybersecurite/

Une loi française votée en 2022 concerne la mise en place d'un Cyber score. Ce label, sur le même principe que le Nutri-Score, devait informer le grand public sur le niveau de sécurisation des données des grandes plateformes après un audit de l'Anssi. Pour l'instant, le décret d'application n'a pas été publié.

Source: (https://www.usine-digitale.fr/article/plus-de-trois-ans-apres-son-adoption-le-cyberscore-n-est-toujours-pas-applicable.N2230274)

6 . RESSOURCES SUPPLÉMENTAIRES

6.1 GLOSSAIRE DES TERMES TECHNIQUES

ANSSI : L'Agence Nationale de la Sécurité des Systèmes d'Information est un service national français rattaché au secrétaire général de la défense et de la sécurité nationale. Son rôle est d'établir des règles de protection des systèmes d'information, mais également de détecter et réagir aux attaques informatiques. https://www.ssi.gouv.fr/

APPAREIL : Le mot appareil est ici utilisé pour désigner indistinctement tout téléphone, tablette ou ordinateur communiquant avec un objet connecté à travers une application.

AUTHENTICITÉ : L'authenticité est un des 4 principes de base de la sécurité de l'information, elle garantit que l'information provient bien de la source qui prétend l'avoir émis. Une information dont l'authenticité n'est pas vérifiée peut provenir d'un pirate qui essaie de se faire passer pour quelqu'un d'autre.

AUTHENTIFICATION : Une authentification est un procédé permettant de s'assurer de l'identité de l'entité avec laquelle on communique. Cela revient dans le monde réel à vérifier la carte d'identité d'une personne.

CERTIFICAT : Un certificat peut être vu comme une carte d'identité numérique, c'est un ensemble de données (nom, adresse électronique, signature numérique ...) servant à prouver l'identité de l'entité qui le présente.

CERTIFICATION : Une certification est un gage de qualité obtenue en remplissant un certain nombre de critère. Obtenir une certification de respect de la vie privée pour un produit indique par exemple au consommateur que ses données ne seront pas utilisées à des fins commerciales ou malicieuses.

CHIFFREMENT : Le chiffrement est un procédé permettant de rendre illisible des données aux personnes non autorisées à les consulter (les personnes ne possédant pas la clé de déchiffrement). Il permet d'assurer la confidentialité et l'intégrité des communications.

CLÉ DE CHIFFREMENT : La clé est le paramètre utilisé dans un algorithme de chiffrement permettant de rendre les données illisibles. Dans le cas d'un algorithme de chiffrement symétrique, la clé de chiffrement fait aussi office de clé de déchiffrement et doit donc rester secrète, alors que dans le cas d'un algorithme asymétrique la clé de chiffrement est publique tandis que la clé de déchiffrement ne doit être connue que du destinataire. La robustesse d'un chiffrement repose en grande partie sur la longueur de ses clés.

CNIL : La Commission Nationale de l'Informatique et des Libertés est une autorité française chargée de s'assurer que l'informatique ne porte pas atteinte aux libertés individuelles, à la vie privée ou encore aux droits de l'Homme. https://www.cnil.fr /

COMPROMISSION : On parle ici de compromission d'un système lorsqu'une personne non autorisée parvient à en prendre le contrôle ou à récupérer les données qu'il contient. Un système compromis n'est pas digne de confiance.

CONFIDENTIALITÉ : La confidentialité est un des 4 principes de base de la sécurité de l'information, elle

assure qu'une information communiquée n'est accessible qu'aux personnes autorisées.

CRYPTOGRAPHIE : La cryptographie est la discipline consistant à chiffrer des messages, c'est-à-dire les rendre illisibles. Elle n'empêche pas d'intercepter les messages, mais ceux-ci sont totalement incompréhensibles tant qu'ils n'ont pas été déchiffrés.

FAILLE : Une faille ou vulnérabilité est une faiblesse dans la conception d'un système qui permet à un assaillant d'exploiter des fonctionnalités pour lesquelles il n'a théoriquement pas l'accès.

FORCE BRUTE : L'attaque par force brute est le type d'attaque le plus basique pour trouver un mot de passe ou une clé, il consiste simplement à tester toutes les possibilités jusqu'à trouver la bonne. Utiliser une clé suffisamment longue permet d'allonger le temps nécessaire pour trouver la bonne, mais il existe des techniques pour accélérer l'attaque, il est donc judicieux de toujours mettre en place des mécanismes contre les attaques par force brute.

HACKER : Un hacker est une personne cherchant à connaître les mécanismes et le fonctionnement des systèmes qu'il utilise. Le terme tel qu'il est utilisé dans ce guide désigne un « grey hat », c'est-à-dire une personne qui recherche des failles sans en avoir l'autorisation et donc généralement illégalement, mais sans pour autant chercher à les exploiter. Le terme hacker ne doit pas être confondu avec pirate.

OBJET CONNECTÉ : Un objet est dit connecté si sa fonction première ne nécessite aucune interaction avec son environnement, mais que l'ajout d'une connexion internet lui apporte une valeur ajoutée. Dans ce guide, on désigne par objet connecté, ou simplement objet, le produit qui est ciblé par une attaque ou qui présente une faille.

PIRATE : Pirate est le terme populairement utilisé pour désigner un hacker « black hat », c'est-à-dire un hacker qui cherche à s'introduire dans un système à des fins malveillantes. Dans ce guide, le terme pirate est utilisé pour désigner un attaquant qui cherche à nuire à l'entreprise.

RGPD : Applicable depuis le 25 mai 2018, le RGPD (pour Règlement Général sur la Protection des Données) est le règlement européen de référence concernant le traitement des données personnelles et la responsabilisation des acteurs au cours de ce traitement.

SENSIBILITÉ DES DONNÉES : La sensibilité d'une donnée correspond au niveau de préjudice qu'elle pourrait porter à l'entité concernée et le degré de confidentialité qu'on souhaite lui apporter. Un pseudonyme est une donnée peu sensible puisqu'il est toujours public, contrairement à un mot de passe qui doit à tout prix être gardé secret et est donc une donnée très sensible. Les informations personnelles comme l'origine, la santé, l'opinion politique et l'orientation sexuelle (entre autres) sont des données sensibles.

SESSION : La session est l'ensemble des actions qu'effectue l'utilisateur sur une application entre le moment où il se connecte et celui où il se déconnecte de l'application.

SURFACE D'ATTAQUE : La surface d'attaque est l'ensemble des vulnérabilités pouvant être exploitées par un pirate pour attaquer un équipement informatique. Pour pouvoir lancer une attaque, il est au préalable nécessaire d'étudier la surface d'attaque pour trouver des failles exploitables.

(Source : IOTRUST, GUIDE DE BONNES PRATIQUES DÉVELOPPEMENT DE SYSTÈME IOT, 2018)

6.2 RESSOURCES SUPPLÉMENTAIRES (LIENS, LECTURES RECOMMANDÉES)

6.2.1 GRAND PUBLIC

"La sécurité des objets connectés (IoT)" par Cybermalveillance.gouv.fr

- Grand public : Ce guide présente dix bonnes pratiques pour sécuriser l'utilisation des objets connectés, telles que changer les mots de passe par défaut, mettre à jour régulièrement les appareils et désactiver les fonctionnalités inutilisées.
  CYBERMALVEILLANCE.GOUV.FR

"Cyber Guide Famille" par le Ministère de l'Intérieur

- Grand public : Ce guide offre des conseils pratiques pour protéger les familles contre les cybermenaces, en abordant des sujets tels que la protection des données personnelles, la sécurisation des appareils et la sensibilisation des enfants aux risques en ligne.
  Ma Sécurité

https://www.fondation-maif.fr/up/pj/20180612_BBU_Guide-bonnes-pratiques-V7_WEB.pdf

6.2.2 ENTREPRISES

https://www.pensezcybersecurite.gc.ca/fr/ressources/internet-des-objets-trousse-dinformation-pour-les-petites-et-moyennes-entreprises

https://www.cyberpreventys.com/blog/securiser-objets-connectes-2/

https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2024/liot-cheval-de-troie-pour-la-cybersecurite-des-entreprises/

6.2.3 TECHNIQUE

"Recommandations relatives à la sécurité des (systèmes d')objets connectés" par l'ANSSI

- Professionnels (conception) : Ce document fournit des recommandations pour sécuriser les systèmes d'objets connectés, en abordant des aspects tels que l'architecture sécurisée, la gestion des données et la maintenance en condition de sécurité.
  Cybermalveillance

"La cybersécurité de vos objets et systèmes connectés" par CAP'TRONIC

- Professionnels (conception) : Ce guide se concentre sur la protection de la chaîne de valeur des objets connectés et des passerelles de communication, en offrant des conseils sur la sécurisation matérielle, les applications et les protocoles de communication.
  CAP'Tronic

Cybersécurité des systèmes industriels
Écrit par Jean-Marie Flaus et publié par ISTE Editions en janvier 2019, ce livre aborde la maîtrise de la cybersécurité des systèmes industriels. Il couvre le fonctionnement des systèmes informatiques, des réseaux de communication, des systèmes de contrôle-commande, les méthodes d'attaque, les normes, la réglementation et les solutions de sécurisation. Il s'adresse aux responsables industriels et aux professionnels de la cybersécurité.
ISTE Group

https://www.istegroup.com/en/produit/cybersecurite-des-maisons-intelligentes/ Mai 2024

https://www.nae.fr/guide-cybersecurite/

https://6113121.fs1.hubspotusercontent-na1.net/hubfs/6113121/White%20Papers%20-%20SMILE%20website%20FR/[FR]%20Livre%20Blanc%20S%C3%A9curit%C3%A9%20des%20Objets%20Connect%C3%A9s%20-%202023.pdf (2023)

https://www.isit.fr/documents/2074/eo_wp-security_v1.0.1.pdf (2022)

https://fr.digi.com/blog/post/embedded-systems-cybersecurity-regulations
https://fr.digi.com/resources/library/white-papers/emerging-medical-device-cybersecurity-legislation

https://www.routledge.com/Security-Engineering-for-Embedded-and-Cyber-Physical-Systems/Motahhir-Maleh/p/book/9781032235462

https://www.m2m.fr/securite/securite-iot/

https://exed.centralesupelec.fr/actualites/cybersecurite-et-iot-enjeux-menaces-et-solutions-partie-1-2/

→ https://www.enisa.europa.eu/news/enisa-news/iot-cybersecurity-webinar-series-to-tackle-security-challenges-of-iot

7 . HISTORIQUE DU DOCUMENT

VERSION	DATE	MODIFICATIONS
V1.0	Octobre 2025	Version diffusable du document.