Comment sécuriser ses achats sur Internet ?

Publié le 09 Janv 2023

achat sécurisé internet achat sécurisé sur internet comment sécuriser ses achats sur internet

Temps de lecture : 11 min

SOMMAIRE

Internet a révolutionné la manière dont nous achetons. Souvent, l'offre pléthorique de produits, aux prix excessivement bas et donc alléchants, et la simplicité d'utilisation des sites d'achat, nous rendent le clic facile... Trop facile ?

Parmi les nombreux sites d'achat se dissimulent parfois, plus ou moins habilement, des vendeurs malveillants qui peuvent vous coûter bien plus cher que le produit initialement désiré. Comment sécuriser alors ses achats sur internet ? Découvrez 5 bonnes pratiques essentielles pour éviter les arnaques et escroqueries.

1. Méfiez-vous des offres trop alléchantes en termes de prix

Il n'est pas rare d'être attiré par des prix particulièrement bas sur Internet. C'est malheureusement parfois le point de départ d'escroqueries. Avant même de penser à acheter votre produit, pensez donc à **comparer son prix sur différents sites web**. Il est fort probable qu'un produit high-tech neuf vendu à 10% de sa valeur originelle, ou qu'un objet extrêmement recherché par les consommateurs à prix cassé cache en fait une arnaque. Après avoir fait ces comparaisons, si l'offre vous semble trop belle pour être vraie, il est recommandé de ne pas procéder à l'achat du produit.

2. Comment sécuriser ses achats sur internet : Vérifiez en amont l'autorité du site web

Dans un second temps, il est nécessaire de bien étudier le site web sur lequel se trouve le produit qui vous intéresse. Il est en effet recommandé de **privilégier des achats sur des sites liés à des sociétés françaises ou de l'Union Européenne.** La raison est simple : il existe une réglementation européenne qui s'applique à ces sites en cas de litige et qui vous protège.

Sachez également que la loi française oblige les détenteurs de sites web e-commerce français (associés à une entreprise créée en France) à mettre à disposition des visiteurs **deux pages clés :**

- **Les Conditions Générales de Vente (CGV)** : elles indiquent les conditions de vente, de reprise, ou encore de retour des produits vendus ;
- **Les Mentions Légales** : elles vous précisent qui se trouve derrière le site web.

Sur un site d'achat fiable, vous trouverez généralement ces deux éléments dans le pied de page du site web (tout en bas de chaque page). Ils vous dévoileront des informations phares sur la fiabilité du site. Des vérifications plus profondes peuvent, cependant, être utiles.

Sur un site e-commerce que vous ne connaissez pas, il est recommandé de **taper dans un moteur de recherche le nom du site vendeur, suivi du mot "arnaque" ou "escroquerie"**. Vous tomberez alors sur des sites où des particuliers auront peut-être déjà signalé des tentatives d'escroqueries ou d'arnaques.

Sachez cependant que même sur un site connu, vous n'êtes malheureusement pas à l'abri. Lorsque vous naviguez sur ce type de site, **vérifiez que vous êtes bien sur l'adresse web (URL) du site officiel**. Elle est affichée dans le navigateur. Certains escrocs sont en effet capables de reproduire l'apparence d'un site bien connu de bout en bout, pour tromper les visiteurs.
Également, s'il s'agit d'un site de type "place de marché" où des vendeurs individuels peuvent proposer leurs produits, veillez à **vérifier l'engagement du site si vous avez des soucis avec le vendeur**. Certains d'entre eux stipulent, dans leurs Conditions Générales de Vente, qu'il est possible de se retourner contre le site si vous rencontrez un problème avec un vendeur individuel.
En règle générale, s'il n'est pas possible de vérifier tous les éléments relatifs au site sur lequel vous êtes, évitez de procéder à l'achat.

3. Vérifiez l'identité du vendeur si vous êtes sur un site "place de marché"

Sur les sites de type « place de marché », comment vous assurer que le vendeur (un individu ou une société) n'a rien de suspicieux ? Vous pouvez procéder à la même vérification que celle mentionnée ci-dessus. **Tapez le nom du site associé au nom du vendeur ainsi qu'au mot "arnaque" ou "escroquerie"** dans un moteur de recherche. Les résultats vous permettront de savoir si ce vendeur a déjà été mis en cause dans des arnaques.

Après avoir vérifié sur votre moteur de recherche si le vendeur a déjà ou non tenté d'arnaquer un autre utilisateur, veillez à :

- **Privilégier les annonces qui donnent une adresse mail et un numéro de téléphone.** Cela vous permet d'appeler le vendeur avant votre achat pour vous assurer de son sérieux.
- **Préférer les annonces où vous pouvez récupérer votre produit en main propre** et payer le vendeur en face à face.

Quelle que soit l'attractivité du produit que vous désirez, il est recommandé de ne pas procéder à l'achat si vous avez le moindre doute sur le vendeur.

Guide des achats en ligne

Réalisé par la Fevad et l'INC, ce guide accompagne les consommateurs tout au long du processus d'achat en ligne et leur donne de précieux conseils pratiques notamment sur le choix des site marchands.

Publié le 14/01/2020
PDF 2 Mo

TÉLÉCHARGER

4. Comment sécuriser ses achats sur internet : Menez quelques vérifications de base au moment de payer

Votre choix est fait, place au paiement. Connaissez-vous vraiment les bonnes pratiques pour être sûr d'éviter le piratage de votre carte bancaire, ou tout simplement comment sécuriser ses achats sur internet ?

Tout d'abord, sachez que **le consentement de paiement en ligne se fait, légalement, par deux clics.**

1. Le premier clic

Vous arrivez sur une page de vérification de la commande, dans laquelle les produits demandés, leur quantité, leur prix, le mode de livraison, et d'autres éléments clés seront rappelés. Vérifiez attentivement toutes ces informations et faites également attention à ce que d'autres options supplémentaires, que vous ne désirez pas, n'aient pas été rajoutées automatiquement (assurances, livraison payante...).

2. Le second clic confirmera effectivement la commande

Pour le paiement, procédez à deux vérifications de sécurité : la première consiste à vérifier que l'adresse web (URL) du site comporte impérativement **la mention "https://" et non "http://"**. Le -s à la fin est symbole de sécurité : il s'agit du protocole TLS, qui garantit le chiffrement de vos données bancaires entre votre machine et le site marchand. L'idée est bien d'éviter le piratage de votre carte bancaire. Vérifiez également l'affichage, près de l'URL, d'**un pictogramme en forme de cadenas** : voilà un signe de sécurité de paiement en ligne.

Attention :

Ce petit cadenas et le « https:// » **ne sont pas un gage de confiance totale de ce site web**. Ils indiquent simplement que la communication entre vous et ce site web est chiffrée. Ne vous limitez donc pas à cette seule vérification et faites preuve de vigilance.

5. Privilégiez les moyens de paiement les plus sécurisés

Pour véritablement vous assurer d'éviter toute fraude, vous pouvez privilégier **les moyens de paiement en ligne type Paylib ou e-Carte Bleue.** Ils vous évitent de communiquer vos informations bancaires au vendeur et vous proposent, dans certains cas, des remboursements ou des annulations de débit si vous rencontrez un litige.

Si vous utilisez votre carte bancaire, on ne doit jamais vous demander plus que quatre éléments, à savoir : votre numéro de carte, le nom associé au compte bancaire, la date de validité de la carte et le cryptogramme à trois chiffres situé au dos de la carte. Ne communiquez en aucun cas le code PIN, qui vous sert à retirer de l'argent au distributeur ou à payer avec votre carte.
Bien souvent, les sites web (même fiables) enregistreront votre numéro de carte bancaire après avoir validé votre commande. **Si vous n'allez pas régulièrement sur ce site, supprimez votre numéro de carte bancaire** pour qu'il ne tombe pas un jour dans de mauvaises mains.

Enfin, n'oubliez pas : même si tout s'est bien passé, après avoir confirmé votre commande, surveillez attentivement votre compte bancaire. Le paiement effectué doit correspondre au montant de l'achat. Vérifiez par ailleurs que de nouvelles opérations que vous n'auriez pas effectuées ne soient pas débitées.

Avec toutes ces vérifications, vous faites le maximum pour éviter arnaques et escroqueries et fiabiliser vos achats sur Internet.

A LIRE AUSSI

Soldes, Black Friday, achats de fin d'année : 7 conseils pour éviter les cyber-arnaques

Voir l'actualité

Avez-vous trouvé cet article intéressant et utile ?

NON OUI

INSCRIVEZ-VOUS À LA NEWSLETTER

Tenez-vous informé(e) de l'actualité de la cybermalveillance et des nouvelles menaces

Entrez votre adresse email

À PROPOS

Qui sommes-nous ?

Kit de communication

Mentions légales

Politique de confidentialité

DIVERS

Plan du site

Presse

Marchés publics

Label ExpertCyber

NOUS SUIVRE

Escroquerie au détournement de loyer

Publié le 10 Janv 2024

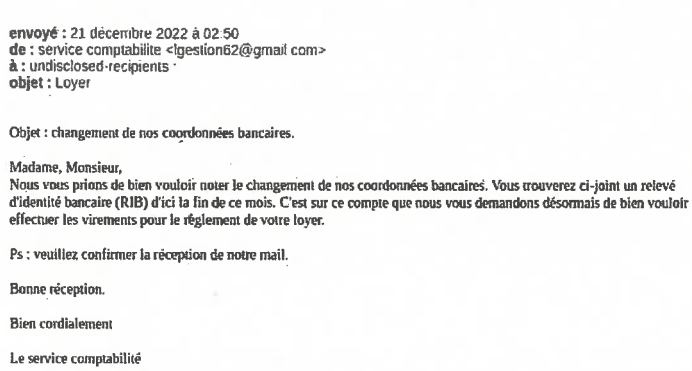
Temps de lecture : 10 min

SOMMAIRE

Vous avez reçu un message (mail) qui semble provenir de votre propriétaire/bailleur ? Il vous annonce un changement de coordonnées bancaires pour le paiement de votre loyer et éventuellement un impayé que vous devez régulariser sans tarder ? Prenez le temps de vérifier ces informations par vous-même, car il peut s'agir d'une tentative d'escroquerie !

Depuis fin 2022, Cybermalveillance.gouv.fr a constaté plusieurs vagues de mails frauduleux supposément émis par des propriétaires/bailleurs. Ces messages cherchent à tromper des locataires afin de détourner le paiement du loyer de leur logement au profit d'escrocs.

Exemples de messages :



envoyé : 21 décembre 2022 à 02:50
de : service comptabilite <lgestion62@gmail com>
à : undisclosed-recipients
objet : Loyer

Objet : changement de nos coordonnées bancaires.

Madame, Monsieur,
Nous vous prions de bien vouloir noter le changement de nos coordonnées bancaires. Vous trouverez ci-joint un relevé d'identité bancaire (RIB) d'ici la fin de ce mois. C'est sur ce compte que nous vous demandons désormais de bien vouloir effectuer les virements pour le règlement de votre loyer.

Ps : veuillez confirmer la réception de notre mail.

Bonne réception.

Bien cordialement

Le service comptabilité

De: "COMPTABILITE.LOYER" <benokosilibe00@gmail.com>
Date: 7 décembre 2022 à 10:58:43 UTC+1
À: undisclosed-recipients:;
Objet: PAIEMENT.EN.RETARD

Bonjour,

A ce jour, sauf erreur de notre part, nous restons dans l'attente du règlement de votre loyer.

En effet, conformément au contrat de location signé, l'échéance pour le paiement étant atteint, je vous remercie de procéder au plus vite au règlement afin de régulariser votre situation de façon amiable.

Nous vous informons par la même occasion de la mise à jour de nos coordonnées bancaires.

N'hésitez pas à répondre directement à ce courrier pour toute demande d'informations complémentaires.

Cordialement,

Service comptabilité

Cet article revient sur ce phénomène et prodigue des conseils pour y faire face.

1. De quoi s'agit-il ?

Dans un message qui semble provenir de votre propriétaire/bailleur ou de son service « comptabilité », vous êtes informé d'un défaut de paiement ou d'un changement de coordonnées bancaires pour le règlement de votre loyer. En général, ce message, assez sommaire, a pour accroche principale un impayé de loyer ou une supposée relance à ce sujet. Il peut également s'agir d'un prétendu changement de raison sociale du bailleur mais, dans chaque variante, vous êtes invité à régulariser cette situation au plus vite. Les arguments employés visent à créer un sentiment d'urgence et d'inquiétude pour vous faire réagir le plus rapidement possible.

Il est important de noter que ce message a un caractère impersonnel. En effet, il ne précise pas votre identité, ni l'adresse de votre logement. L'identité ou la raison sociale du propriétaire/bailleur n'est également pas mentionnée.

Dans certains cas observés, les escrocs prétextent un problème de comptabilité pour demander le paiement du loyer en coupons PCS que les victimes doivent acheter chez un buraliste.

Il s'agit d'une **tentative d'arnaque** qui a pour **objectif de vous soutirer de l'argent**.

2. Que faire si vous recevez ce message ?

1/ **Ne répondez pas** ! Ce message à caractère impersonnel est une arnaque envoyée par vague à des milliers de personnes dont l'adresse mail a pu être trouvée sur Internet. Vous n'êtes donc pas personnellement concerné.

2/ **Ne payez pas** ! Vous alimenteriez un système criminel et resteriez redevable du véritable paiement de votre loyer à votre propriétaire/bailleur.

3/ Au moindre doute, **contactez votre propriétaire/bailleur par vos moyens habituels pour confirmer ou infirmer le message reçu.** Vous trouverez ses coordonnées sur vos quittances de loyer ou tout autre document lié à la location de votre logement.

4/ **Signalez le message frauduleux** à Signal Spam. Vous contribuerez ainsi à la lutte contre ce phénomène cybercriminel.

5/ **Signalez la tentative d'escroquerie** sur la plateforme dédiée du ministère de l'Intérieur (Pharos) : Internet-signalement.gouv.fr.

3. Et si vous êtes victime ?

Si vous avez payé, vous êtes victime d'une **escroquerie**, au sens de l'article 313-1 du Code pénal : délit passible de cinq ans d'emprisonnement et de 375 000 euros d'amende.

1/ Alertez immédiatement votre banque de l'opération frauduleuse pour tenter de suspendre le virement si celui-ci n'est pas encore effectué. Dans le cas contraire, demandez le retour des fonds. Votre banque pourra exiger une copie de votre dépôt de plainte pour instruire votre demande.

2/ Conservez les preuves ! Conservez les messages reçus (mails...), les coordonnées bancaires de l'escroc, etc., et toute autre information qui pourront vous servir pour signaler les faits et déposer plainte.

3/ En parallèle des démarches auprès de votre établissement bancaire, déposez plainte au commissariat de police ou à la brigade de gendarmerie ou par écrit au procureur de la République du tribunal judiciaire dont vous dépendez en fournissant toutes les preuves en votre possession.
Vous pouvez être accompagné gratuitement dans cette démarche par l'association France Victimes au 116 006 (appel et service gratuits), qui opère le numéro d'aide aux victimes du ministère de la Justice. Service ouvert 7 jours sur 7, de 9h à 19h.

4/ Pour être conseillé dans vos démarches, contactez la plateforme Info Escroqueries du ministère de l'Intérieur au 0 805 805 817 (appel et service gratuits). Le service est ouvert de 9h à 18h30 du lundi au vendredi.

Extraits de messages frauduleux :

Objet : ***Règlement loyer***

Bonjour,

sauf erreur de notre part, nous restons dans l'attente du règlement de votre loyer mensuel.

– –

Objet : *Re: RELANCE POUR LOYER IMPAYÉ*

Bonjour,

A ce jour et sauf erreur de notre part, nous vous rappelons que nous n'avons toujours pas réceptionné votre paiement pour le loyer de ce mois.

Si vous l'avez deja réglé, merci de nous joindre une preuve de paiement (bordereau, ordre de virement).

– –

Objet : ***Quittance de loyer***

Bonjour Mme / Mr

Sauf erreur de notre part, nous restons dans l'attente du règlement de votre loyer mensuel.

Merci de bien vouloir régulariser votre situation à réception de votre mail.

Nous vous informons par la même occasion de la mise à jour de nos coordonnées

bancaires.

En vôtre aimable règlement

N'hésitez pas à répondre directement à ce mail pour toute demande d'informations

complémentaires.

Vous en souhaitant bonne réception de la présente.

Bien cordialement,

– –

Objet : ***<< RAPPEL DE PAIEMENT >>***

Madame, Monsieur,

À ce jour et sauf erreur de notre part, nous vous rappelons que nous n'avions toujours pas réceptionné votre paiement pour le loyer du mois.

En effet, nous venons par ce message vous informer de la mise à jour de nos références bancaire.

Aussi, nous vous remercions de procéder le plus rapidement possible pour régler cette échéance afin de régulariser votre situation...

– –

Objet : ***Locataire***

Bonjour,

pour cette nouvelle année nous vous informons qu'une mise à jour a été effectué au sein de notre établissement de ce fait nous avons apporté quelques changements au niveau de la comptabilité

un nouveau RIB pour les paiements locatifs.

Veuillez confirmer que vous avez bien reçu nos emails afin de vous envoyer vos coordonnées bancaires avant votre prochain paiement mensuel...

A LIRE AUSSI

Campagne de messages frauduleux réclamant le paiement d'une contravention

Voir l'actualité

La sécurité des objets connectés (IoT)

Publié le 12 Nov 2020

ioT objets connectés Sécurité des objets connectés

Temps de lecture : 15 min

SOMMAIRE

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

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. Ce conseil est également applicable à l'ensemble des appareils de votre réseau numérique.

3. Mettez à jour sans tarder vos objets connectés et les applications associées

« Pourquoi dit-on mot de passe et pas mot de passoire ? » – Vidéo réalisée en partenariat avec le groupe France Télévisions

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.

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 observaient et parlait à l'enfant pour l'effrayer quand elle était seule.

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.

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.

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.

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.

En 2018, un casino s'est fait pirater la base de données de ses plus gros clients. Les pirates ont réussi à y accéder en passant par le

thermomètre connecté insuffisamment sécurisé d'un aquarium de l'établissement.

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.

9. Limitez l'accès de vos objets connectés aux autres appareils électroniques ou informatiques

« Appareils numériques : pourquoi faut-il faire ses mises à jour » – Consomag réalisé en partenariat avec l'Institut National de la Consommation.

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.

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.

Pour aller plus loin :

– Par l'ANSSI : Recommandations relatives à la sécurité des systèmes d'objets connectés

Nos supports sur la sécurité des objets connectés

La sécurité des objets connectés (IoT)

Appliquez nos 10 recommandations pour utiliser au mieux vos objets connectés en sécurité grâce à notre fiche pratique consacrée au sujet.

Publié le 12/03/2021
PDF 430 Ko

TÉLÉCHARGER

La sécurité des objets connectés (IoT) en fiche mémo

Retrouvez la synthèse de la fiche pratique sur la sécurité des objets connectés (IoT) au format mémo.

Publié le 12/03/2021
PDF 289 Ko

TÉLÉCHARGER

Pour informer et sensibiliser les publics sur les menaces numériques, Cybermalveillance.gouv.fr met à disposition divers contenus thématiques : des supports variés pour comprendre les cybermenaces et savoir comment y réagir, ainsi que des bonnes pratiques à adopter pour assurer votre cybersécurité.
> Consulter la liste de l'ensemble des ressources mises à disposition par le dispositif.

DIAGNOSTIQUER UN INCIDENT

Vous pensez être victime d'un piratage ou d'une attaque informatique ?

DÉMARRER UN DIAGNOSTIC

Avez-vous trouvé cet article intéressant et utile ?

NON OUI

AUTRES BONNES PRATIQUES

Pourquoi et comment bien gérer ses mots de passe ?
23/11/2019 Temps de lecture : 19 min

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise... La sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur...

Pourquoi et comment bien gérer ses mises à jour ?

26/11/2019 Temps de lecture : 16 min

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'une...

Les 10 mesures essentielles pour assurer votre cybersécurité

06/01/2021 Temps de lecture : 16 min

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Cette intensification des usages représente pour les cybercriminels une...

INSCRIVEZ-VOUS À LA NEWSLETTER

Tenez-vous informé(e) de l'actualité de la cybermalveillance et des nouvelles menaces

Entrez votre adresse email