# Informatique & Internet

## S'ÉQUIPER ET NAVIGUER en toute SÉCURITÉ

GENERALI

# Informatique & Internet

## S'ÉQUIPER ET NAVIGUER en toute SÉCURITÉ

GENERALI

163 milliards de téraoctets

C'est le volume **DE DONNÉES INFORMATIQUES** que l'humanité **devra stocker à l'horizon 2025,** selon la société d'analystes IDC, soit **10 fois plus qu'en 2016.**

# Informatique & Internet

## S'ÉQUIPER ET NAVIGUER en toute SÉCURITÉ

**Depuis 25 ans, Internet révolutionne les modes de vie des Français. Des enfants aux seniors, tout le monde est concerné et, qu'il s'agisse de navigation ou d'équipement informatique, chacun d'entre nous s'expose, souvent sans le savoir, à des risques pourtant faciles à maîtriser avec quelques bonnes pratiques.**

Selon le Baromètre du numérique publié par le Crédoc (Centre de recherche pour l'étude et l'observation des conditions de vie) en 2017, 76 % des Français de plus de 12 ans se connectent à Internet tous les jours ! Dans le détail, 67 % effectuent des démarches administratives, 61 % ont réalisé au moins un achat en ligne et 59 % sont inscrits sur un réseau social (Facebook, Instagram...). Sans compter que les outils pour se connecter ne manquent pas. Depuis une dizaine d'années, en plus de l'ordinateur, ces services sont accessibles depuis une tablette ou un téléphone.

### Tous concernés

« Il faut prendre le train de la sécurité en marche et embarquer toute la famille », insiste Jérémy Verrier, responsable de la sécurité des systèmes d'information (RSSI) chez Generali France. Comme beaucoup de parents, cet expert s'inquiète que les enfants et les jeunes, nés avec ces outils, n'en mesurent pas pour autant tous les dangers. « Eux comme nous devons prendre de bonnes habitudes dès que possible. C'est indispensable car Internet va continuer de prendre une place de plus en plus grande dans nos vies. »

Imaginez-vous voir un jour votre ordinateur bloqué par un pirate avec une demande de rançon ? Sans doute pas, et pourtant cela arrive, même à des particuliers. « Il faut tout anticiper pour ne pas subir », insiste Jérémy Verrier. En 2018, il a justement participé à la 18e édition des Assises de la sécurité autour de cette question. « Nous aurions tort de penser que les ransomwares (logiciels malveillants prenant en otage des données personnelles)

## Le boom à venir **des objets connectés**

Lentement mais sûrement, l'Internet des objets (IoT, «Internet of Things») s'installe lui aussi dans nos vies. Selon l'institut Gartner, ce marché, encore naissant, devrait devenir la norme d'ici cinq ans, lorsque 15% de tous les objets seront concernés. Les ordinateurs, les tablettes, les téléphones ne sont déjà plus les seuls objets connectés de notre quotidien. Voitures, montres et même réfrigérateurs peuvent également être connectés. Avec, au passage, d'autres dangers pour notre vie privée : sous couvert d'améliorer notre quotidien, ces appareils engrangent en effet des données très personnelles sur notre santé, nos déplacements, nos activités. Or ces objets sont encore loin d'être totalement sécurisés…

sont passés de mode ou ne concernent que des entreprises. Tout utilisateur d'ordinateur s'expose à des risques et à des dangers.» Mots de passe ou mises à jour régulières : lui-même confie qu'il est particulièrement vigilant. Car aucun appareil n'est à l'abri : «L'expérience montre que 50 % des problèmes viennent d'équipements mal entretenus et mal protégés. Quant aux 50 % restants, ils sont causés généralement par l'utilisateur lui-même, souvent imprudent car insuffisamment sensibilisé.»

**73 %**
**des Français**

de plus de 12 ans **possèdent un smartphone.** Une croissance exponentielle : en 2011, seuls 17 % en avaient un.

Source : Baromètre du numérique du Crédoc, 2017.

**4 h 48**

**C'est le temps moyen passé** sur Internet chaque jour, dans l'Hexagone, **dont 1 h 22 sur les réseaux sociaux,** selon l'enquête « Le digital en France », réalisée en 2018 par We Are Social. Ces chiffres concernent **les 88 % de Français** qui ont accès à une connexion.

# VRAI ou FAUX

**Prêt à tester vos connaissances numériques ?**

**Évaluez-vous et jouez avec vos proches. Retrouvez les solutions ci-dessous et, si vous avez quelques points à réviser, rendez-vous dans les pages qui suivent.**

| | VRAI | FAUX |
|---|---|---|
| **1** Les objets connectés ne peuvent pas subir d'attaque informatique (p. 6) | ○ | ○ |
| **2** Je n'éteins jamais complètement mon ordinateur : cela optimise ses performances (p. 7) | ○ | ○ |
| **3** Poser mon appareil sur mes draps ou mes genoux risque d'endommager la ventilation (p. 8) | ○ | ○ |
| **4** Réinitialiser le système d'origine efface toutes mes données (p. 9) | ○ | ○ |
| **5** Un pavé tactile (trackpad) est meilleur pour le poignet et la main qu'une souris (p. 10) | ○ | ○ |
| **6** Le numéro IMEI permet de bloquer mon téléphone à distance (p. 12) | ○ | ○ |
| **7** Activer régulièrement les mises à jour permet de corriger les vulnérabilités (p. 13) | ○ | ○ |
| **8** La lumière du téléphone augmente la production de mélatonine, l'hormone du sommeil (p. 14) | ○ | ○ |
| **9** Le hameçonnage (phishing) peut prendre la forme d'un faux mail administratif (p. 16) | ○ | ○ |
| **10** Je peux me connecter sans danger aux Wi-Fi publics, ils sont tous sécurisés (p. 17) | ○ | ○ |
| **11** Pour ne pas être soumis à des publicités ciblées, je supprime mon historique de navigation (p. 18) | ○ | ○ |
| **12** J'utilise une messagerie cryptée pour éviter l'interception et le stockage de mes données (p. 19) | ○ | ○ |
| **13** Je dispose de 14 jours pour me rétracter après un achat en ligne (p. 20) | ○ | ○ |
| **14** L'utilisation accompagnée d'Internet est recommandée à partir de 6 ans (p. 22) | ○ | ○ |
| **15** La baisse des résultats scolaires peut trahir une exposition excessive aux écrans (p. 23) | ○ | ○ |
| **16** Si mon enfant est cyberharcelé, je prends les devants et réponds pour lui (p. 24) | ○ | ○ |

Réponses 1 : F - 2 : F - 3 : V - 4 : V - 5 : F - 6 : V - 7 : V - 8 : F - 9 : V - 10 : F - 11 : F - 12 : V - 13 : V - 14 : F - 15 : V - 16 : F


# À la MAISON

**Plus de 80 % des Français de 12 ans et plus disposent aujourd'hui d'un ordinateur à la maison et 33 % déclarent même avoir plusieurs appareils pour se connecter à Internet. Autant d'objets à protéger…**

Imaginiez-vous leur espérance de vie si courte ? Aujourd'hui, la durée d'utilisation moyenne d'un ordinateur dépasserait rarement cinq à six ans pour un fixe et seulement trois à quatre ans pour un portable[1] ! Les raisons pour changer de matériel sont variées : pannes, retards au démarrage, lenteur de certains logiciels… ou encore casse et vol. Pourtant, beaucoup de ces mésaventures pourraient être évitées…

## Vers plus de sécurité

Mieux vaut anticiper, car le préjudice financier, déjà non négligeable, est loin d'être le seul. C'est non seulement une perte de temps, mais aussi une source de stress. C'est généralement le moment où l'on se souvient que l'ordinateur contient toutes ses photos de famille, sa comptabilité ou encore sa musique préférée et sa collection de films et de séries. Si, finalement, le matériel doit être changé, il faudra aussi prévoir du temps et de l'énergie pour réinstaller ses logiciels. Sans avoir de connaissances très poussées en informatique, mais en adoptant quelques mesures simples, vous éviterez de sérieux tracas et vous ferez peut-être quelques économies !

**1 491 €/an**

C'est le **budget moyen par foyer français** consacré aux **produits technologiques** (nouveaux appareils, réparations et abonnements).

Source : Les Français et leur budget technologies, sondage OpinionWay pour Sofinco, baromètre Sofinscope, février 2018.

1. Cabinet Wipro Technologies.

# SOIGNER son installation

**Avant même de vous connecter à Internet, commencez par protéger vos différents appareils. Pour les garder longtemps comme pour prévenir d'éventuelles intrusions.**

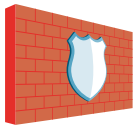

## Protégez l'ordinateur par un mot de passe

Faites-le lors de sa configuration initiale. Vous pouvez aussi l'ajouter plus tard ou le changer dans vos paramètres.

## Sécurisez votre Wi-Fi

Choisissez l'option WPA sur l'interface de gestion de votre box pour ajouter une clé de cryptage.

• ➤ Ce mot de passe empêchera des inconnus d'utiliser votre réseau (et de télécharger des fichiers illégalement par exemple).



## Ayez un pare-feu et un antivirus

S'ils ne figurent pas dans les logiciels fournis avec l'ordinateur, ajoutez-les.

• ➤ Complémentaires, ils bloquent toute tentative d'intrusion malveillante et détectent les virus.

## Préférez les produits reconditionnés

Si vous optez pour du matériel d'occasion, achetez des ordinateurs remis dans leur configuration « d'usine ».

## Pensez aux consoles de jeux

Ce sont aujourd'hui des miniordinateurs qui peuvent être des portes d'entrée dans votre Wi-Fi. Protégez-les par des mots de passe. Côté jeux, proscrivez les contrefaçons, qui pourraient endommager l'appareil.

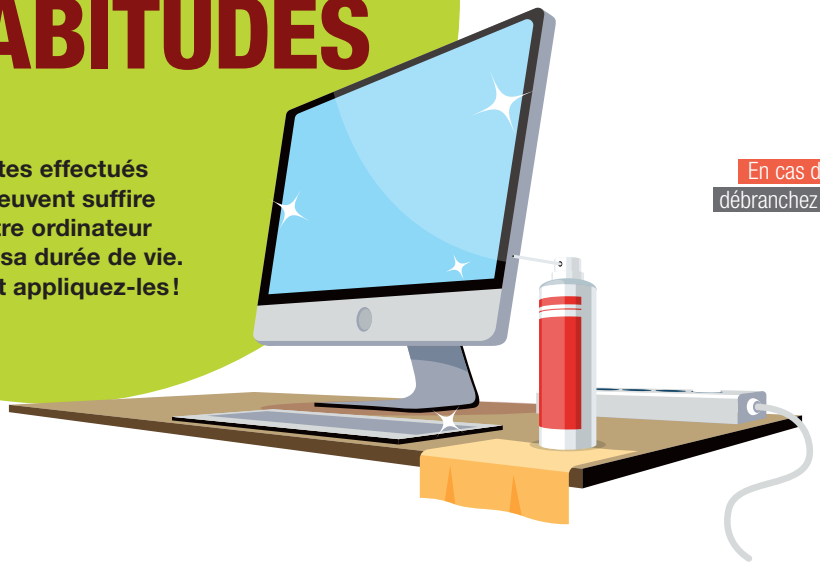
**80 % DES OBJETS CONNECTÉS NE SERAIENT PAS TESTÉS POUR RÉSISTER À UNE ATTAQUE INFORMATIQUE* !**

Tout ce que vous connectez à Internet (enceinte, jouet pour enfant ou encore brosse à dents) est **une porte d'entrée potentielle vers vos données.** Sécurisez ces objets avec un mot de passe et évitez de les connecter à un réseau public. Enfin, faites des mises à jour fréquentes.

* Étude sur la sécurité des applications IoT publiée en 2017 par Arxan et IBM.

# Prendre de bonnes HABITUDES

**Quelques gestes effectués chaque jour peuvent suffire à protéger votre ordinateur et augmenter sa durée de vie. Retenez-les et appliquez-les !**



## Utilisez une multiprise parafoudre

Votre ordinateur sera ainsi protégé des surtensions, des variations de courant et de la foudre.

En cas d'orage, débranchez tous vos appareils informatiques.

## Contactez un dépanneur

Si votre appareil est sous garantie et même après, ayez toujours à portée de main, en cas de panne, le numéro de votre service après-vente ou d'un réparateur certifié ainsi que votre facture d'achat.

## Ne traînez pas dans vos mises à jour

Elles peuvent intégrer une protection supplémentaire pour votre ordinateur. Mais vérifiez toujours au préalable leur compatibilité.

## Éteignez vos appareils le soir

Vous ferez des économies d'énergie. Fermer complètement l'ordinateur de temps en temps permet d'activer les mises à jour automatiques, de refroidir l'appareil et d'augmenter ses performances.

## Nettoyez-les régulièrement

Avec un chiffon microfibre, un nettoyant sans alcool et une bombe à air sec, dépoussiérez votre écran et les interstices de votre clavier.

### OPTIMISEZ LA MÉMOIRE

- **Désinstallez les programmes** non utilisés qui ralentissent votre équipement.
- **Archivez vos fichiers.** Compressés, leur taille va considérablement diminuer.
- **Videz les dossiers oubliés.** Faites ponctuellement un tour du côté des dossiers préconfigurés vidéos, téléchargements ou musique et effacez régulièrement le contenu de la corbeille.

# Adopter de bons réflexes

**Qui veut utiliser son matériel longtemps ménage son équipement en évitant une chute, une surchauffe… Voici quelques astuces pour ne pas s'arrêter en bon chemin.**

## Évitez les surchauffes

Laissez votre ordinateur portable ventiler et ne le posez pas sur vos genoux ou vos draps : vous risquez d'obstruer les prises d'air.

• ➤ Le système de refroidissement de votre ordinateur portable est fragile et a besoin d'être ménagé.

Pour les ordinateurs portables, il existe des platines refroidissantes qui complètent le système d'aération.

## Éloignez tout liquide de votre appareil

En cas d'accident, vous risquez d'altérer vos données et d'endommager les composants de votre ordinateur.

• ➤ Ne mangez pas devant votre ordinateur car les miettes pourraient dégrader les circuits.

## Prenez soin de vos câbles

Pour débrancher votre ordinateur, ne tirez pas sur le câble, vous risquez de le casser ou d'abîmer la prise.

• ➤ Fixez-le avec de l'adhésif pour vous éviter de marcher ou de rouler dessus avec un fauteuil à roulettes !

## Attention aux animaux de compagnie

Tenez-les éloignés autant que possible de vos appareils pour éviter tout accident. Leurs poils pourraient s'introduire dans l'appareil.

### TRANSPORTER SON ORDINATEUR PORTABLE

- **Ne le laissez pas au soleil,** même l'écran fermé : vous pourriez endommager les processeurs.
- **Habillez-le d'une coque** ou utilisez un sac rigide : les portables sont vulnérables et sensibles aux chocs.

### LE SAVIEZ-VOUS ?

**Vider complètement puis recharger la batterie au moins une fois tous les deux mois permettra d'augmenter sa durée de vie.**

# Sauvegarder ses données

**Un ordinateur cassé ou volé, c'est une mauvaise nouvelle. Si l'on songe à tous les documents qui y sont conservés, c'est encore plus stressant. N'attendez pas qu'il soit trop tard et anticipez, au cas où…**


## Utilisez un disque dur externe

C'est utile pour mettre à l'abri des documents importants ou des photos de famille.

## Stockez vos documents dans un cloud

Cette solution, gratuite ou payante selon le volume souhaité, permet de sauvegarder ses données sur un serveur distant et donc de les récupérer à tout moment sur n'importe quel ordinateur.

## Chiffrez vos documents personnels

Des logiciels gratuits comme AxCrypt ou 7Zip permettent de sécuriser n'importe quel fichier confidentiel. Il devient ainsi illisible en cas de vol ou d'intrusion.

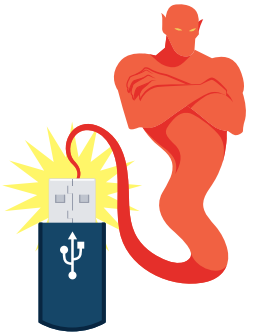
### FAITES UNE COPIE DE VOTRE SYSTÈME ENTIER

Cette fonctionnalité (à renouveler idéalement une fois par mois) prend quelques heures mais permet de graver **sur un disque dur externe la totalité de son ordinateur,** logiciels comme fichiers, pour pouvoir les réinstaller à l'identique en cas d'incident.

## Faites attention à ce que vous branchez

N'utilisez jamais une clé USB trouvée. Avant de la connecter, vous devez être sûr de sa provenance car elle pourrait contenir un logiciel espion ou endommager votre système.

• ➤ De même, ne laissez pas un inconnu charger son téléphone sur votre ordinateur. Attention au risque d'aspiration des données contenues dans votre appareil !



## Nettoyez votre ordinateur si vous le vendez

En réinitialisant le système d'origine, vous effacez vos données personnelles.

# Préserver sa santé

**Avec le nombre d'heures passées devant les écrans, il n'est pas inutile de prévenir, chez soi comme au bureau, certains risques physiques dus à une utilisation prolongée des ordinateurs. Là aussi, suivez quelques précautions élémentaires.**

Une exposition excessive aux écrans peut être facteur de stress.
Il est conseillé de prendre 15 minutes de pause toutes les 2 heures.


## Utilisez une souris plutôt qu'un pavé tactile

Branchée à un portable, la souris limite la fatigue au niveau du poignet et de la main.

## Désinfectez votre matériel

Utilisez un désinfectant sans alcool : clavier, souris et casque peuvent vite devenir des nids à microbes.

## Protégez-vous des ondes

Bien qu'il n'y ait aucune certitude sur le sujet, il est recommandé, si vous êtes équipé d'une borne Wi-Fi, de l'installer en dehors des chambres et de la débrancher la nuit.

## Prenez la bonne posture

À la maison comme au bureau, privilégiez un fauteuil à hauteur réglable pour toute utilisation continue d'un ordinateur.
Position idéale : les pieds à plat, les coudes à 90°, les poignets flottants, le dos droit et l'écran de 10 à 20° au-dessous de la hauteur des yeux.
Et évitez l'ordinateur portable sur le canapé ou au lit.

### SOIGNEZ VOS YEUX

Pour y voir clair et éviter les maux de tête, placez vos écrans **perpendiculairement aux fenêtres.** Cela limitera les reflets. Sinon, fermez les stores et privilégiez un éclairage artificiel. En cas de picotements ou d'yeux rouges et secs, **faites des pauses,** utilisez des gouttes hydratantes et envisagez des lunettes adaptées à la lumière bleue des ordinateurs.

### LE SAVIEZ-VOUS ?

**Une mauvaise posture peut engendrer sur le long terme des troubles musculo-squelettiques (TMS) et toucher muscles et tendons de la nuque, des épaules, de la région lombaire, des poignets et des mains.**

# Smartphones ET TABLETTES

**Dans 40 % des cas de vols violents,** l'objet convoité était **un téléphone portable,** selon le rapport annuel 2017 de l'ONDRP (Observatoire national de la délinquance et des réponses pénales).

**Un Français sur deux se connecte aujourd'hui à Internet avec un smartphone ou une tablette, plus faciles à perdre qu'un ordinateur, et remplis de données tout aussi sensibles. Raison de plus pour redoubler d'attention !**

Voilà une maladie, on ne peut plus réelle, qui n'existait pas encore il y a dix ans : la nomophobie. C'est la peur panique de sortir sans son téléphone. Elle en dit long sur la place que le mobile a prise dans la vie de chacun. À la question « quel équipement utilisez-vous le plus souvent pour vous connecter à Internet ? », 42 % des Français répondaient en 2017 « un smartphone » et 7 % « une tablette »[1].

## Des objets plus polyvalents

Si ces usages augmentent, c'est justement parce que les téléphones mobiles notamment ne servent plus seulement à téléphoner ! Ils ont remplacé les appareils photo (et même les albums) ainsi que les carnets d'adresses. Ils donnent accès à la boîte mail et aux réseaux sociaux. Leurs applications permettent aussi de consulter le compte en banque ou de payer les impôts. Bref, ils savent absolument tout de la vie de leur utilisateur. Perdre son téléphone, c'est aujourd'hui s'exposer à un double embarras : devoir remplacer un accessoire onéreux mais aussi disperser dans la nature des données souvent très personnelles. Protégez-vous avant qu'il ne soit trop tard…

1. Baromètre du numérique, réalisé par le Centre de recherche pour l'étude et l'observation des conditions de vie (Crédoc).

# Prévenir le vol

**De plus en plus légers et perfectionnés, les smartphones et les tablettes sont devenus pour beaucoup des accessoires indispensables. Mais il ne faut jamais perdre de vue que ces précieux objets suscitent aussi la convoitise.**

## Choisissez un rangement sécurisé

La première des précautions est de bien ranger ses appareils pendant ses déplacements.

• ➤ Évitez par exemple les poches extérieures ou les sacs à dos.

## Prenez une photo du voleur

Des applications de sécurité permettent de faire retentir une alarme à distance, de localiser son smartphone, mais aussi… de prendre et de vous envoyer une photo de quiconque saisit plusieurs fois un mot de passe erroné.

## Verrouillez-les avec un code

Sur un smartphone ou une tablette, ce code de 4 chiffres empêchera de les utiliser en cas de vol. À condition de ne pas choisir 1234, 0000 ou son année de naissance…

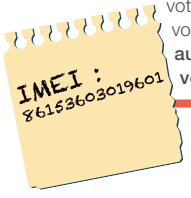
## Activez la géolocalisation

Située dans les paramètres généraux, cette fonction proposée par de plus en plus d'appareils permet de localiser son téléphone en temps réel sur une carte.

### BLOQUER SON TÉLÉPHONE À DISTANCE

L'**IMEI** (International Mobile Equiment Identity) est le **numéro d'identité de votre appareil.** Le noter en lieu sûr vous permettra, en cas de vol, de **bloquer à distance l'utilisation de votre téléphone portable sur l'ensemble des réseaux mobiles.**

Composé de 15 à 17 chiffres, il est inscrit sous la batterie de votre téléphone portable et sur le coffret que vous recevez lors de l'achat. **Vous pouvez aussi l'obtenir en tapant le code *#06# sur votre smartphone.**



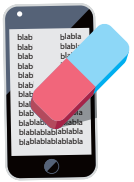
# Protéger ses données

**Contacts, photos, documents, voire coordonnées bancaires : les possesseurs de smartphone stockent des données à caractère privé ou sensible. Autant de raisons de sécuriser votre matériel contre le piratage.**

## Gardez vos appareils à jour

Activez régulièrement les mises à jour proposées pour le téléphone ou la tablette, comme pour leurs applications. Cela permet de corriger en temps réel des vulnérabilités observées.

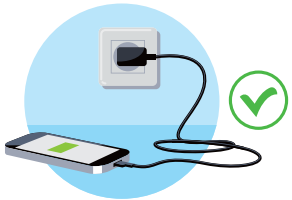
## Réinitialisez votre téléphone



Si vous vous en séparez, comme pour un ordinateur, mieux vaut vider la mémoire pour effacer tous vos contacts et fichiers.

## Choisissez bien vos applications

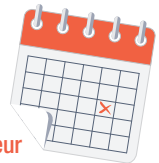
Ne téléchargez que ce qui vous semble nécessaire et, surtout, désactivez l'accès à vos données personnelles (votre répertoire par exemple) quand il n'est pas indispensable au fonctionnement de l'application, notamment pour les jeux.



## Ne rechargez pas votre smartphone n'importe où

En panne de batterie, il peut paraître tentant, dans un train par exemple, de recharger son smartphone sur l'ordinateur portable d'un inconnu. Or vous courez le risque de voir toutes vos données aspirées en quelques minutes.

## Sauvegardez vos données



Vous pouvez télécharger vos fichiers sur un ordinateur et/ou les enregistrer dans un cloud sécurisé pour les récupérer en cas de problème ou de vol.

## COMMENT RÉAGIR EN CAS DE VOL DE DONNÉES

Si l'espoir de retrouver son téléphone est perdu, **mieux vaut effacer les données qu'il contient.** La plupart des téléphones ont une fonctionnalité intégrée («Effacer» sous Android ou Windows Phone, «Effacer toutes mes données» chez Samsung ou «Effacer l'iPhone» pour Apple), activable à distance depuis son interface iCloud, Windows Phone ou depuis le site de son opérateur.

# Penser à sa santé et à sa sécurité

**Si les smartphones et les tablettes facilitent souvent la vie, ils apportent aussi leur lot de dangers insoupçonnés. Adoptez quelques gestes simples pour ne pas (trop) nuire à votre sécurité.**

L'écoute prolongée avec des écouteurs peut contribuer à fatiguer votre système auditif.

## Déconnectez à la maison

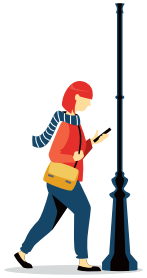
Attention au stress que ces appareils génèrent dans la vie de famille. Plus d'une personne sur deux s'est déjà disputée avec son conjoint à cause de l'utilisation d'un smartphone à table ou pendant une conversation.

## Jamais avant de dormir

La lumière dégagée par un téléphone ou une tablette ralentit la production de mélatonine, c'est-à-dire l'hormone du sommeil. Vous risquez alors de vous endormir moins vite.

## N'utilisez pas votre téléphone au volant

La loi interdit désormais de téléphoner ou de consulter son smartphone en conduisant. L'utilisation d'un mobile diminue la vigilance et augmente donc le risque d'accident.

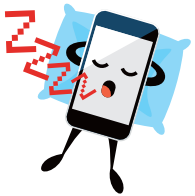


## À pied aussi, soyez prudent

La consultation de son téléphone est une cause d'accidents de plus en plus fréquente chez les piétons (chutes, collisions).

## Activez le mode « avion »

Difficile de se passer de son smartphone, qui sert souvent de réveil. Le mode « avion » coupe les appels, les messages, la connexion Wi-Fi et les données cellulaires du téléphone ainsi que les ondes qu'il émet, mais pas le réveil !



## LE SAVIEZ-VOUS ?

**Des applications comme Off Time peuvent vous aider à prendre conscience du temps passé devant vos écrans et ainsi à le réduire.**


# Sur INTERNET

**1 million**

C'est le nombre **de personnes abusées** chaque année par de faux sites administratifs. **Un vol de 150 millions d'euros** selon la DGCCRF.

(Direction générale de la concurrence, de la consommation et de la répression des fraudes)

**Le piratage, qui se décline en phishing, en ransomware ou encore en vol de données, touche autant les particuliers que les entreprises. Voire davantage, car l'installation et la maintenance des appareils à la maison sont rarement faits par des professionnels.**

Pour inciter à naviguer sur le web avec plus de prudence et renforcer la prise de conscience, le gouvernement a lancé en octobre 2017 le portail cybermalveillance.gouv.fr. Premier bilan : parmi les attaques signalées au cours des six premiers mois, 84 % visaient des particuliers et seulement 16 % des professionnels ou des collectivités ! Qu'il s'agisse d'attaques ciblées ou non, les intrusions sont multiples. Cela n'arrive pas qu'aux autres…

## Un seul clic et tout peut basculer

Qui n'a pas déjà reçu un mail à entête d'une administration connue (en apparence seulement), invitant à ouvrir un lien suspect pour obtenir un remboursement par exemple ? Attention, si cela vous arrive, un seul clic pourra suffire à paralyser votre ordinateur ! Ou, pire encore, à héberger, sans le savoir, un hacker qui pillera tranquillement vos données personnelles ou détournera vos comptes. Mais il ne suffit pas de se méfier des pirates, il faut aussi se montrer prudent, en ne diffusant pas à la légère des informations personnelles, sur les réseaux sociaux notamment, pour ne pas aider les escrocs 2.0. Des habitudes très simples à prendre vous aideront à protéger votre vie privée et à éviter des risques inutiles.

# Éviter les pièges classiques

**Sur le web ou les réseaux sociaux, il est possible de lire son courrier, regarder un film, déclarer ses impôts ou discuter avec des amis, ce qui n'est pas sans risque. Adoptez quelques réflexes nécessaires pour vous en prémunir.**

## Faire face au ransomware

Si votre ordinateur et vos données sont pris en otage contre une demande de rançon ne payez surtout pas. Déconnectez vos appareils des réseaux et portez plainte auprès de la police nationale ou de la gendarmerie.

- ➤ Vous pouvez également signaler les faits sur la plateforme Pharos.
- ➤ Réinitialisez ensuite votre ordinateur afin de supprimer le virus.

## Reconnaissez vos amis

Sur les réseaux sociaux, n'acceptez pas n'importe qui parmi vos contacts car vous leur ouvrez ainsi votre carnet d'adresses.

## Méfiez-vous des fausses applications

Attention aux arnaques. Avant de télécharger une application, vérifiez le nom de son développeur (Facebook pour Messenger par exemple).

- ➤ Regardez aussi le nombre d'avis et les notes sur les plateformes de téléchargement.

## Décelez les faux sites administratifs

Leur but est généralement de facturer des actes gratuits ou de diffuser de fausses infos. Les faux sites peuvent se terminer par .org ou .gouv.com. Les officiels, eux, finissent exclusivement par .gouv.fr ou .fr. Dans le doute, service-public.fr vous orientera vers les sites de référence.

- ➤ https://www.internet-signalement.gouv.fr permet de signaler les arnaques afin d'éviter que d'autres ne tombent dans le même piège.

## Résistez au phishing

Ces attaques courantes, aussi appelées hameçonnage, consistent à envoyer de faux mails (aux couleurs de la Sécurité sociale par exemple) proposant un remboursement imaginaire. Surtout ne répondez pas et n'entrez jamais vos coordonnées bancaires.

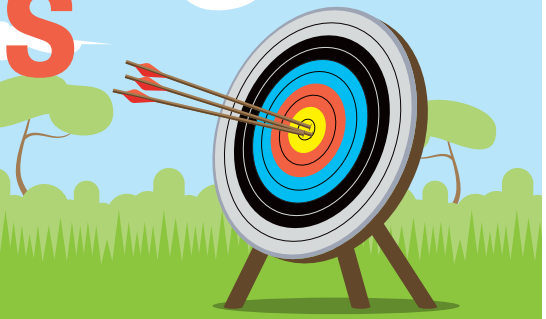
Téléchargez sur des sites officiels !
Le piratage est un vol pour lequel vous pouvez être poursuivi et qui vous expose à de dangereux virus.

## 3 INDICES D'UN FAUX « APPEL AU SECOURS »

- Vous recevez un message ou un mail avec des fautes d'orthographe inhabituelles.
- Il parle d'argent (en demande en urgence ou promet de vous en donner).
- Il vous engage à ouvrir une pièce jointe (drôle ou à caractère sexuel) ou à contacter quelqu'un.

**N'envoyez jamais d'argent, ne donnez pas vos coordonnées personnelles ou bancaires, n'ouvrez jamais de pièce jointe suspecte ou inattendue sans avoir vérifié l'identité de votre interlocuteur.**

# Parer aux attaques ciblées



**Il suffit de peu pour que votre usage d'Internet et vos habitudes de navigation laissent échapper certaines de vos informations personnelles. Quelques précautions s'imposent.**


## Choisissez un mot de passe solide

Si vous ouvrez un compte sur un site, soyez attentif à votre mot de passe. N'utilisez pas le même sur tous les sites et changez-en souvent.

• ➤ Idéalement, écrivez-le en 12 caractères avec des minuscules, des majuscules, des chiffres et des caractères spéciaux.
• ➤ La CNIL propose un générateur qui permet de concevoir un mot de passe en quelques secondes : www.cnil.fr/fr/generer-un-mot-de-passe-solide

## Veillez à vos informations personnelles

Pour ne pas être importuné ou piraté, mieux vaut ne pas laisser traîner son numéro de téléphone, son adresse, voire son mail personnel sur des sites (réseaux sociaux ou forums).

Placez un autocollant sur votre webcam afin d'empêcher toute prise de contrôle extérieure.

## Faites attention aux Wi-Fi publics

En déplacement, ne vous connectez surtout pas au premier réseau libre. Choisissez-en un doté d'un système de mot de passe ou d'identification.

• ➤ Même sur un Wi-Fi public ou identifié, abstenez-vous de faire transiter toute donnée trop personnelle ou confidentielle.

## Ne donnez pas les réponses de vos mots-clés

Évitez de dévoiler sur un site public le nom de votre chat ou de la ville où vous êtes né. Ce sont souvent des réponses à des « questions secrètes » utiles pour pirater un compte.

## N'aidez pas les cambrioleurs

Évitez de communiquer vos dates de congés sur les réseaux sociaux et de publier vos photos. Vérifiez dans vos paramètres que seuls vos amis ont accès à vos publications et que votre géolocalisation est désactivée.

## Sécurisez vos comptes

Ajoutez un numéro de téléphone dans vos paramètres de sécurité. Si votre adresse mail ou votre page Facebook est piratée, ce sera alors plus facile de prouver votre identité et de la récupérer.

### PHOTOS : EFFACEZ VOS DONNÉES PERSONNELLES

Quand vous prenez une photo, le fichier contient souvent **des « métadonnées » très personnelles (nom, localisation, date et heure, matériel utilisé…).** Avant de poster une photo, vous pouvez retirer ces informations en cliquant sur l'onglet Propriétés.

# Naviguer SANS être tracké

**Les navigateurs et les marques collectent et conservent vos informations. Quelques conseils pour garder le contrôle de vos données et éviter d'être submergé par les relances commerciales.**

## Déconnectez-vous !

Pourquoi, lorsque vous effectuez une recherche sur votre ordinateur, une publicité ciblée apparaît-elle sur votre téléphone ? L'historique de vos recherches est associé à vos comptes connectés à l'instant où vous naviguez (session Google, Facebook, Apple, Android…). Déconnectez-vous régulièrement, de vos comptes sur vos différents appareils.

## Surfez en « privé »

Cette option à activer dans votre navigateur, y compris dans Google, permet de ne pas enregistrer une partie de vos données comme les pages visitées, les cookies, les données de formulaires… et ainsi de réduire le ciblage publicitaire.


Même si vous refusez le tracking publicitaire, vous recevrez toujours des publicités mais elles ne seront plus adaptées à vous ni à vos intérêts.

## Ne dites pas tout à Google

Il enregistre les données personnelles que vous lui fournissez (mots de passe, champs de formulaires…) ainsi que vos données de navigation via les cookies (sites visités, achats effectués, fichiers téléchargés…). Certains de ces éléments peuvent ensuite être utilisés à des fins publicitaires en vous proposant du contenu personnalisé.

- ➤ Utilisez des antipublicités comme Adblock afin de les bloquer ou Ghostery pour empêcher la collecte de données.
- ➤ Les moteurs de recherche sécurisés DuckduckGo ou Qwant affirment protéger la vie privée de leurs utilisateurs (pas de pistage ni de cookies).

## Effacez les cookies

Les sites marchands et les sites de marques conservent des informations comme vos préférences et vos historiques de navigation pour déterminer votre « profil comportemental ». Effacez-les régulièrement (dans les paramètres de votre navigateur).

- ➤ Vous pouvez aussi configurer votre navigateur pour qu'il vous prévienne et que vous ayez l'option de les rejeter ou de les bloquer automatiquement.
- ➤ Installez des logiciels gratuits comme Spybot ou CCleaner, qui effacent toute trace de vos navigations.

## L'EUROPE VOUS DONNE DES DROITS GRÂCE AU RGPD

Les entreprises n'ont plus le droit de faire n'importe quoi avec vos données personnelles. **Avec le RGPD, vous pouvez par exemple, en toute sécurité et très simplement, changer de compte mail et récupérer tous les renseignements de ce dernier,** recueillir et transférer vos informations d'une banque à une autre, **demander la suppression de vos données du fichier d'une marque ou d'une entreprise** (adresse mail, coordonnées postales et bancaires, date de naissance, préférences...). De plus, **les éventuels recours sont facilités** et les conditions d'utilisation sur les sites clarifiées. Retrouvez plus d'informations sur le site de la CNIL.

# Préserver sa vie privée et sa réputation

**Donner des nouvelles ou un avis, comme partager une information ou ses photos de vacances, rien de plus facile ! À tel point que nous oublions parfois de réfléchir avant d'appuyer sur la touche «publier». Mais avez-vous pensé à toutes les conséquences ?**


## Soignez votre réputation sur le Net

Internet n'oublie rien et certaines traces peu valorisantes sont difficiles à effacer. Évitez donc de poster des photos de vous, vous pourriez le regretter plus tard.

• ➤ De même, gardez pour vous ou pour des messageries privées certains états d'âme. N'oubliez jamais qu'un employeur ou des clients par exemple pourront aussi retrouver ces informations.

## Protégez aussi les autres

Attention aussi à ce que vous publiez et partagez sur les autres, textes comme photos. Toute violation de leur vie privée ou publication d'une information fausse ou préjudiciable vous expose à des poursuites.

## Vérifiez vos paramètres de confidentialité

Sur les réseaux sociaux, assurez-vous que vos publications sont réservées uniquement à vos amis et qu'elles n'apparaissent pas en mode public.

### LE DROIT À L'OUBLI, COMMENT ÇA MARCHE ?

La loi vous autorise à demander **la suppression d'informations vous concernant** sur Internet (nom, adresse, photos, etc.) à condition d'avoir un motif « légitime » (atteinte à sa vie privée ou à sa réputation par exemple). Un modèle de courrier est disponible sur le site de la CNIL (www.cnil.fr).

## Utilisez une messagerie cryptée

À l'inverse des messageries traditionnelles, les messages, photos, vidéos, extraits audio échangés y sont chiffrés via une clé d'encodage et peuvent difficilement être interceptés et stockés par les éditeurs, les fournisseurs d'accès Internet, les autorités.

• ➤ Quelques-unes à considérer : Signal, Telegram, WhatsApp, iMessage, Bleep, Wickr, Keeply…

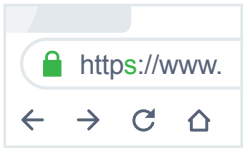
### LE SAVIEZ-VOUS ?

**Certaines messageries disposent d'un service de cryptage mais ne l'installent pas par défaut. Pour en bénéficier, il suffit d'activer l'option « chiffrement de bout en bout » sur Facebook Messenger, Skype…**

# Effectuer des achats en ligne

**Plus d'un Français sur deux réalise aujourd'hui une partie de ses courses en ligne. Si le e-commerce est de plus en plus sécurisé et encadré par le Code de la consommation (art. L221-1), des précautions s'imposent malgré tout.**

Créez une adresse mail juste pour vos achats afin de protéger votre vie privée et d'éviter de crouler sous les offres commerciales.




## Sécurisez votre paiement

**L'adresse doit commencer par « https://... » avec un cadenas fermé dans le haut de la fenêtre du navigateur.**

• ➤ Vous pouvez aussi utiliser un moyen de paiement alternatif : Paypal ou carte bancaire virtuelle.

## VOUS POUVEZ CHANGER D'AVIS !

Une fois la livraison effectuée, vous disposez de **14 jours pour vous rétracter,** sans vous justifier, et simplement renvoyer l'achat à vos frais pour être remboursé. Cela est valable **en France comme en Europe** pour une majorité de sites. Attention, il existe des exceptions sur le droit de rétractation de certains produits ou services. Renseignez-vous sur le site du Centre européen des consommateurs (CEC).


## Lisez bien les conditions générales de vente

Elles figurent en général en bas de la page d'accueil. Privilégiez, si possible, des sites français ou européens pour éviter des droits de douane ou de TVA supplémentaires et faciliter d'éventuels recours.

## Repérez les arnaques

L'affaire paraît trop belle ? Attention, il peut s'agir d'une contrefaçon ou d'une escroquerie. Avant un achat, vérifiez, pour les entreprises françaises, sur societe.com, qu'il s'agit bien d'une véritable entreprise.

• ➤ Pour les transactions entre particuliers, privilégiez les sites offrant une garantie, rencontrez physiquement votre interlocuteur, exigez un paiement par cash et choisissez un envoi suivi.

## LE SAVIEZ-VOUS ?

**Vous pouvez vous faire aider en cas de litige. Contactez d'abord le service client du vendeur. Si cela ne marche pas, vous pouvez recourir à une médiation gratuite sur www.economie.gouv.fr/mediation-conso ou vous faire aider par le CEC.**

# Avec les ENFANTS

**Les écrans sont désormais omniprésents dans la vie de tous y compris des plus jeunes. Se divertir, apprendre, communiquer…bien utilisés, les outils numériques peuvent avoir des vertus pédagogiques. Mais certains excès provoquent des effets insoupçonnés sur la santé, le développement et l'équilibre émotionnel des enfants et des adolescents.**

Il n'est plus rare aujourd'hui de voir un enfant jouer dès son plus jeune âge avec le smartphone ou la tablette de ses parents. Or c'est souvent l'exposer, sans le savoir, à de nombreux effets indésirables. Saviez-vous que la lumière bleue émise par les écrans affecte la synthèse de mélatonine, indispensable au mécanisme du sommeil. À l'adolescence, elle favoriserait même la myopie ! Une étude publiée en 2017 par l'Inserm confirme aussi un lien entre le temps passé devant les écrans et le surpoids. D'autres évoquent des troubles de la concentration voire des risques d'addiction, entre autres. Pourtant, réfléchir au bon usage de ces appareils permettrait d'en garder le meilleur. Adopter et transmettre quelques bonnes pratiques peut aider à protéger les enfants et les accompagner dans la maîtrise des outils.

## Un contrôle indispensable à tout point de vue

Ces chiffres ont fait frémir beaucoup de parents : selon l'association e-Enfance, 40 % des enfants ont déjà été témoins ou victimes de violences en ligne. Pire encore, 22 % des victimes cyberharcelées n'en parlent à personne. Parfois, cela mène à la dépression, voire au suicide. En cause : l'utilisation, mal maîtrisée, des nouvelles technologies de communication, et en particulier des téléphones et des réseaux sociaux.

**23 %**

des 11-14 ans **peuvent rester debout la nuit** ou même se réveiller pour aller sur Internet. Chez les 15-18 ans, c'est le cas de **41,7 % des filles et de 37,7 % des garçons.**

Source : enquête « Génération numérique » (2016).

# Limiter l'exposition aux écrans

**Parce que les écrans ont pris une place centrale dans les activités des enfants, il devient essentiel d'appliquer certaines règles et bonnes pratiques pour préserver leur santé et leur équilibre émotionnel.**

## Apprenez la règle 3-6-9-12 (ans)

Relayée par l'Association française de pédiatrie ambulatoire (AFPA), elle recommande de limiter l'exposition des enfants aux écrans selon leur âge.

- Avant 3 ans : pas de télévision et des jeux sur tablette accompagnés.
- Entre 3 et 6 ans : usage pour des périodes courtes et pas d'images violentes.
- Avant 9 ans : pas d'Internet.
- Entre 9 et 12 ans : apprentissage des règles de l'activité en ligne et Internet accompagné jusqu'à l'entrée au collège.

## Mettez-les dehors !

Une activité et du sport en plein air diminuent les risques d'obésité. Pour éviter les risques de myopie, exposez vos enfants au maximum à la lumière du jour plutôt qu'aux écrans.

## Évitez certains jouets connectés

Équipés de connexions Bluetooth et Wi-Fi, ces robots et peluches interagissent avec les enfants. Cependant, bien que branchés sur votre réseau, ils demeurent insuffisamment sécurisés, d'où des risques d'intrusion supplémentaires (cf. p.6).

## Imposez des limites

Activez les filtres de contrôle parental sur votre box Internet et coupez votre Wi-Fi la nuit. Interdisez aussi les écrans et les téléphones dans les chambres à coucher.


DONNEZ L'EXEMPLE

**JOUEZ À DÉCONNECTER**

**N'oubliez pas que c'est aussi à vous, parents, de donner le bon exemple** en n'utilisant pas votre smartphone à table par exemple. Pour aller plus loin de façon ludique, vous pouvez aussi télécharger l'application ShutApp, qui lance des défis de déconnexion (exemple : ne pas toucher à son téléphone pendant deux heures).

# Accompagner les adolescents

**Ils accèdent de plus en plus jeunes au téléphone et à la tablette et se servent de l'ordinateur familial. N'hésitez pas à les assister et soyez disponibles pour répondre à leurs questions lors de leurs premiers pas dans le monde connecté.**

## Éduquez vos ados aux risques d'Internet

Expliquez-leur l'intérêt d'Internet, mais aussi ses dangers possibles : confrontation probable à des informations fantaisistes ou non vérifiées, exposition possible à des images violentes ou à de la pornographie, risques de cyberharcèlement, de dépendance aux écrans…

• ➤ À consulter, les messages diffusés par les commissariats d'arrondissement lors des interventions de prévention dans les écoles sur : www.prefecturedepolice.interieur.gouv.fr (Rubrique Vous aider/Vous êtes victime/Atteintes aux personnes/Les dangers de l'Internet).

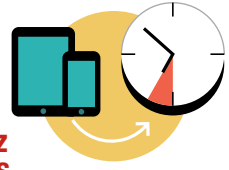
## Soyez présents pour leurs débuts

Sur les réseaux sociaux comme Facebook ou Snapchat, définissez ensemble les paramètres de confidentialité. Négociez aussi un droit de regard sur les publications et les amis virtuels de vos enfants.

• ➤ Évoquez les dérives possibles – par SMS, applications ou via les réseaux sociaux – et engagez-les à vous parler s'ils ont des problèmes.

## Encouragez le bon sens numérique

Apprenez-leur à ne partager aucune information personnelle avec des inconnus, à exercer leur sens critique, à bien réfléchir au poids de leurs mots avant toute publication ou encore à éviter de plagier s'ils effectuent des recherches pour des devoirs.



## Établissez des règles

Définissez ensemble le temps passé sur Internet et sur les jeux vidéo, les horaires de connexion et les sites consultés.

## Soyez attentif à leur sommeil

Une grande fatigue et la baisse des résultats scolaires peuvent être les symptômes d'une trop grande exposition aux écrans.

• ➤ Si le sommeil de votre enfant est décalé, bannissez temporairement téléphone et écrans, dînez à heure fixe et avancez son horaire de coucher jusqu'à ce qu'il retrouve un rythme normal.

## Favorisez leur sociabilité

Encouragez les activités physiques en extérieur et invitez les copains pour les ancrer dans le monde « réel ».

# Faire face au cyberharcèlement

**Rumeurs, intimidations ou encore moqueries : si le harcèlement n'est pas un phénomène récent dans les cours d'école, il a pris d'autres formes avec le développement des nouvelles technologies. Sachez reconnaître les symptômes et agir.**

Brisez le silence : si le cyberharcèlement est avéré, rassurez votre enfant et faites-lui comprendre qu'il n'est pas seul.

## Repérez les signaux d'alerte possibles

Une victime de cyberharcèlement a souvent tendance à se replier sur elle-même. Parmi d'autres indices figurent l'anxiété, la peur, les troubles du sommeil, des retards ou des absences à l'école ou encore des résultats scolaires en baisse.

## Rassemblez des preuves pour agir

Faites des captures d'écran des messages reçus puis signalez-les auprès des modérateurs ou des réseaux sociaux pour les supprimer. Ne cherchez pas à répondre à la place de votre enfant. Si les faits perdurent, remettez-vous-en à la justice. Portez plainte et constituez-vous partie civile.

## Appelez le numéro national gratuit

Joignez Net Écoute au 0800 200 000. Ce service a été mis en place grâce au partenariat entre le ministère de l'Éducation nationale et l'association e-Enfance dans le cadre du programme européen Safer Internet.

## Consultez un psychologue

Si votre enfant est durablement perturbé, il aura besoin d'aide pour surmonter cette épreuve.

**LE SAVIEZ-VOUS ?**

**C'est la fréquence et la teneur insultante des propos qui constituent le harcèlement. Les auteurs sont souvent des connaissances de l'enfant rencontrées par le biais de l'école, d'amis ou d'une activité extrascolaire.**

# Protéger et améliorer la vie de nos clients

## GENERALI EN BREF

Generali France est une filiale du groupe Generali, l'un des principaux groupes mondiaux d'assurance et de services financiers, **accompagnant plus de 55 millions de clients dans plus de 60 pays, avec 73000 collaborateurs à travers le monde.** Par sa solidité financière, sa dynamique d'innovation mais aussi son implantation historique dans l'Hexagone, Generali France compte parmi les principaux assureurs du pays. L'entreprise propose **des produits et des services qui couvrent tous les besoins :** assurance dommages, épargne et protection sociale pour les particuliers, les entreprises ou encore les professionnels… Mais aussi l'assistance grâce à sa filiale Europ Assistance.

**La prévention est au cœur du métier de l'assurance.**

Pour Generali, être assureur, c'est d'abord savoir anticiper les risques, les usages et les besoins.
Cette politique se traduit dans toutes nos activités, en matière d'innovation, de services, mais aussi dans le développement de vastes dispositifs de prévention.
Notre métier est de protéger nos clients et d'améliorer la vie des gens.
Pour cela, la prévention est un levier essentiel permettant tout à la fois de contribuer à l'amélioration de la qualité de vie des assurés et de réduire le coût des dommages.
Ce principe de bon sens s'applique à tous les domaines, notamment en matière de cybersécurité. Il s'agit de développer des réflexes efficaces au quotidien, pour la sécurité et le bien-être de chacun.

# Guide pratique

## Que faire en cas de litige, d'atteinte à votre réputation ou d'usurpation d'identité ?

**Votre vie privée a été dévoilée sur les réseaux sociaux, votre enfant est harcelé ou de fausses informations circulent ?**
Vous faites face à un litige relatif à un achat réalisé sur Internet ? Votre identité a été usurpée ?

►► N'hésitez pas à porter plainte et à solliciter de l'aide.

– Si vous êtes client Generali et que vous avez souscrit le contrat Protection juridique Vie privée :

- ► **Contactez Generali** pour prendre conseil et couvrir vos éventuels frais.
- ► **Une équipe de professionnels** est à votre écoute pour répondre à toute question d'ordre juridique, administratif ou social.
- ► **Des spécialistes sont à vos côtés** pour vous assister dans la défense de vos intérêts, du règlement à l'amiable au recours à une procédure judiciaire.
- ► **Vous bénéficiez d'un accompagnement** téléphonique pour vous aider à remplir vos documents administratifs.
- ► **Un service d'écoute et d'accueil psychologique** est à votre disposition par téléphone.

### CONTACTER GENERALI

- 09 69 32 27 25
- generali.fr/espace-client

## Que faire en cas de vol ?

### Portez plainte auprès de la police ou de la gendarmerie
(pour un ordinateur, munissez-vous de la marque, du modèle, du numéro de série).

- ► **Contactez Generali** et déclarez le vol sous 10 jours ouvrés suivant la date où vous en avez connaissance en joignant une copie du dépôt de plainte. Transmettez dans les 15 jours un état estimatif des dommages accompagné des justificatifs tels que factures, photos et certificats d'authenticité.

### Vous avez été cambriolé

Vous avez souscrit une assurance habitation.

- ► **Avec la garantie Vol-vandalisme : dommages mobiliers,** Generali vous indemnise sur les biens volés ou endommagés dans votre habitation. Cette garantie s'applique à la suite d'une tentative de vol, d'un vol ou d'un acte de vandalisme. Elle ne prend pas en charge le vol, la tentative de vol ou l'acte de vandalisme commis par vos locataires, sous-locataires, colocataires ou toute autre personne hébergée dans l'habitation assurée.
- ► **Avec l'option Valeur de remplacement à neuf,** si vos équipements hi-fi, son, audiovisuels et informatiques ont moins de 5 ans, nous vous indemnisons sur la valeur au prix du neuf le jour du sinistre d'objets identiques ou à caractéristiques et performances équivalentes.

### À l'extérieur

Vous avez souscrit la garantie optionnelle Vol sur la personne dans le cadre de votre assurance habitation. Elle s'applique en France et lors d'un séjour à l'étranger.

- ► **Nous vous indemnisons sur vos objets** ou effets personnels volés ou endommagés si vous êtes victime d'une tentative de vol ou d'un vol par agression à l'extérieur de chez vous.

# Guide pratique

## Que faire en cas de bris de matériel informatique ?

### Contactez Generali et déclarez le sinistre.

Si vous avez souscrit la garantie optionnelle Bris de matériel informatique dans votre assurance habitation :

- **Generali vous indemnise** afin de réparer ou remplacer le matériel endommagé si celui-ci a moins de 5 ans et est cassé accidentellement.

## PROTÉGEZ VOS DOCUMENTS DANS UN COFFRE-FORT ÉLECTRONIQUE

**Europ Assistance,** filiale de Generali, propose le service 123Classez (123classez.com), agréé par la Cnil.

- Ce coffre-fort électronique accueille vos documents importants et vous permet d'y accéder où vous voulez, quand vous voulez, en toute confidentialité et de manière sécurisée.
- Dès le processus d'authentification, l'ensemble des communications avec l'assuré sont cryptées, y compris lorsque vous transférez des documents.

Generali Iard, Société anonyme au capital de 94 630 300 euros - Entreprise régie par le code des assurances - 552 062 663 RCS Paris - Siège social : 2 rue Pillet-Will - 75009 Paris

Société appartenant au Groupe Generali immatriculé sur le registre italien des groupes d'assurances sous le numéro 026.

Création éditoriale et graphique, réalisation et illustration : Accroche-com' - Sauf illustrations d'après Idix : p. 7 : prise - p. 17 : téléphone - p. 23 et p. 24 - Photos : Shutterstock