

Internet

Edition 2017

et vous



Devenir **un internaute averti**

**Ce guide, édité en octobre 2012, a été conçu et réalisé par
l'Association Léo Lagrange pour la défense des consommateurs.**

Réédition 2017

Textes : Philippe Capitaine, Sabine Rossignol,
Ludivine Coly-Dufourt, Amélie Jouve

Illustrations et conception graphique : Maya Lambert



Internet est devenu un outil de communication incontournable et fait partie intégrante de nos vies quotidiennes. Face aux possibilités toujours plus grandes offertes par les Technologies de l'information et de la communication (Internet, téléphone fixe, smartphone, etc.), le consommateur doit être en mesure d'acquérir et de maîtriser une quantité d'informations grandissante.

Dans ce contexte technologique mouvant, l'information et la formation des consommateurs sont donc plus que jamais indispensables, afin de leur faire prendre conscience des avantages et des dangers de cet environnement à la fois utile et hostile.

Dans le cadre de notre mission d'éducation à une consommation plus responsable, l'Association Léo Lagrange pour la défense des consommateurs (ALLDC) s'engage sur cette thématique depuis plusieurs années (protection des données personnelles, commerce électronique, compteurs évolués). Ce guide pratique s'inscrit dans le prolongement de notre action quotidienne et souhaite donner aux consommateurs les clés et repères nécessaires pour une utilisation éclairée des supports numériques et d'Internet. Cet outil pédagogique concerne toutes les tranches d'âge et vise à sensibiliser et accompagner le plus grand nombre de consommateurs en leur donnant des conseils et des astuces pour dialoguer, jouer ou encore acheter sur Internet en toute sécurité et sérénité !

Bonne lecture et soyez vigilants !

Philippe Capitaine

Chargé de Mission Technologies de l'information et de la communication
Administrateur de l'ALLDC

Sommaire



Introduction :	Devenir un internaute averti	p.5
-----------------------	------------------------------	-----

.....

1 La messagerie

1.	Un outil de communication fiable	p.8
2.	Une porte ouverte aux intrusions	p.9
3.	Quelques conseils utiles pour protéger votre e-mail des courriers indésirables	p.10

.....

2 Les réseaux sociaux, forums, blogs et autres messageries instantanées

1.	Contrôlez les informations que vous diffusez	p.17
2.	Respectez la vie privée d'autrui	p.18
3.	Quelques conseils utiles pour bien utiliser ces services	p.22

.....

3 Le téléchargement de fichiers

1.	Les différents types de fichiers téléchargeables	p.26
2.	Et les applications dans tout ça ?	p.27
3.	Quelques conseils utiles avant de télécharger	p.30
4.	Le Cloud	p.32

.....

4 L'achat en ligne

1.	L'achat entre particuliers sur les plateformes de vente	p.36
2.	L'achat sur un site marchand	p.38



Internet a bouleversé les modes de fonctionnement traditionnels de la plupart des sociétés contemporaines. En quelques années, Internet a touché un public de plus en plus nombreux et satisfait des besoins de plus en plus variés, de la mise en réseau de la recherche, au commerce à distance en passant par les services administratifs en ligne ou la communication et le partage de fichiers, photos, documents entre particuliers, sans oublier les utilisations malveillantes (spam), frauduleuses ou délictueuses.

Le saviez-vous ?

Selon Médiamétrie, en 2017, 45.8 millions de Français sont désormais connectés à Internet. 20.3 millions d'entre eux s'y connectent via deux écrans et 17.3 millions via trois écrans.

81.2% des Français utilisent un ordinateur pour se connecter, mais chez les jeunes (moins de 34 ans), ce chiffre a tendance à baisser, au profit des smartphones. Ils sont 96 % à préférer surfer sur leur smartphone.

De plus, depuis quelques années, les objets connectés se sont introduits dans la vie des consommateurs. En France, ce marché est estimé à 150 millions d'euros en 2013 et atteint 500 millions en fin d'année 2016, selon une étude Xerfi du 7 décembre 2015. On en trouve dans le secteur de la santé, du bien-être et de la domotique. Les objets connectés sont des objets, reliés à Internet, capables de communiquer avec d'autres systèmes, pour obtenir ou fournir de l'information.

Pour le consommateur, Internet se présente comme un moyen d'information et de communication très économique et totalement libéré des contraintes de temps et de distance.

Le saviez-vous ?

La loi pour une République numérique du 7 octobre 2016 a prévu un droit au maintien de la connexion Internet pour les foyers vulnérables. En cas de problème de paiement, ils pourront sous certaines conditions bénéficier d'une aide financière via le Fonds social pour le logement (FSL). Cette mesure fait aujourd'hui l'objet d'une expérimentation dans quelques départements. Après évaluation, le FSL numérique pourra être généralisé à l'ensemble du territoire. Renseignez-vous auprès de votre conseil départemental pour savoir si votre département est concerné par l'expérimentation.

Le saviez-vous ?

La technologie Internet a été conçue par les milieux américains de la défense et de la recherche, à la fin des années 1960, puis s'est progressivement généralisée au domaine civil et commercial. Limité à un millier environ en 1985, le nombre d'utilisateurs d'Internet est passé à plus de 2 millions en 1994 à 3,025 milliards d'internautes en 2015, soit 42% de la population mondiale.

Source : La Documentation française et le Blog du Modérateur

Pour l'utilisateur professionnel, il s'agit d'un outil de promotion d'une très grande efficacité et qui permet de réaliser un grand nombre de transactions sans contrainte de calendrier et de situation, comme l'éloignement géographique entre l'utilisateur/client potentiel et l'administration ou l'entreprise.

En effet, Internet, au-delà de la communication classique, autorise le choix entre un système passif, dans lequel il est possible de consulter un nombre infini de sites pour y recueillir des informations, et un système actif, dans lequel il est possible de donner une opinion, de passer des commandes, de jouer en ligne, de créer son propre site, de communiquer en direct avec un ou plusieurs interlocuteurs simultanément par écrit et/ou par la voix et/ou par l'image.

Avec Internet, s'effacent les notions de distance et de temps, c'est un peu comme si nous étions finalement tous voisins dans le même cybermonde.

On voit ainsi s'organiser de nouvelles règles du jeu, par essence internationales et de nouveaux enjeux comme la protection de la vie privée, la sécurisation des données, l'information et la défense des cyberconsommateurs.

Mais quelles sont les pratiques les plus courantes des consommateurs sur Internet, comment les conseiller pour qu'ils apprennent à utiliser ces technologies de manière sécurisée et en toute connaissance de cause ?

Ce guide aborde le téléchargement, la messagerie, le e-commerce, les réseaux sociaux, les objets connectés et constituera nous le souhaitons un outil pédagogique utile pour une utilisation responsable d'Internet.

la Mess@- gerie



La messagerie

La messagerie, appelée également courrier électronique est sans nul doute le service le plus utilisé par les internautes de tous âges et de toutes catégories sociales. Ce service est d'ailleurs né bien avant Internet, en 1965, et servait déjà de moyen de communication entre utilisateurs d'ordinateurs partageant un même réseau interne (intranet). Aujourd'hui, la messagerie permet la transmission de courriers envoyés électroniquement via le réseau Internet. Pour ce faire, l'auteur et le destinataire du message doivent tous les deux disposer d'une adresse électronique.

1) La messagerie : un outil de communication fiable

Les pertes de messages (courriels, mails) sont rares et souvent provoquées par des erreurs de manipulation. La présence de l'interlocuteur n'est pas nécessaire au moment de la réception du message, et le mail donne la possibilité de joindre des documents et autres fichiers de toute nature (vidéos, musiques, photos...).

Elle ne dépend pas d'un logiciel particulier : Il est possible d'utiliser votre messagerie sans logiciel spécifique simplement en allant sur le site du fournisseur de messagerie en utilisant un navigateur Internet. En outre, les logiciels de messagerie électronique existants sont gratuits ou intégrés aux suites bureautiques (Outlook, Thunderbird...).

Elle ne dépend pas de l'équipement utilisé : Votre service de messagerie est accessible depuis n'importe quel ordinateur, tablette ou smartphone connecté à Internet, même si ce n'est pas le vôtre.

2) Une porte ouverte aux intrusions

La messagerie électronique est aussi un moyen efficace et économique de passer des messages de promotion commerciale, d'hameçonnage, de cyber-harcèlement et des messages contenant des virus capables d'endommager votre ordinateur. Ceux qui cherchent à vous envoyer ces types de messages intrusifs ont simplement besoin de votre adresse de messagerie.

A chaque fois que vous laissez votre adresse de messagerie dans un formulaire d'inscription, vous ouvrez une porte et mettez le doigt dans un engrenage mondial extrêmement complexe (une véritable boîte de Pandore). A partir de ce moment, votre adresse de messagerie peut être récupérée par de nombreux moyens, licites et illicites, et donc utilisée à votre insu.

Vous avez dit hameçonnage ?

Le phishing ou hameçonnage est un phénomène mettant en danger la protection des données personnelles des internautes. Il s'agit d'un courrier électronique qui vous envoie sur de faux sites web d'institutions ou de grandes entreprises commerciales, où l'on tentera d'obtenir de vous, numéro de carte de crédit, nom d'utilisateur, mot de passe, numéro de sécurité sociale...

Par exemple, en juillet 2011, des allocataires de la Caisse d'allocations familiales (CAF) ont reçu un mail frauduleux leur annonçant qu'ils bénéficiaient de l'allocation « prime d'aide aux vacances » de 152,45 €. Pour ce faire, il suffisait de retourner une photocopie de leur carte nationale d'identité et un justificatif de domicile. Or, cet envoi permettait aux fraudeurs de créer de fausses cartes d'identité.

Le saviez-vous ?

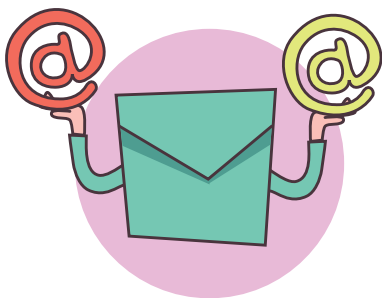
4,4 milliards, c'est le nombre de comptes e-mail répertoriés dans le monde en 2015 (prévision pour fin 2019 : 5,6 milliards)
75 % des comptes sont personnels,
25 % professionnels

Source : Radicati Group, mars 2016

3) Quelques conseils utiles pour protéger votre e-mail des courriers indésirables

Utiliser deux adresses de messagerie

Un moyen efficace de réduire considérablement ce problème est d'utiliser deux adresses de messagerie, l'une dite « publique » et l'autre dite « privée ». L'adresse publique est celle que vous utiliserez lors de vos navigations sur Internet et en particulier sur les formulaires d'inscription. L'adresse privée, quant à elle, ne sera divulguée qu'à vos correspondants privés et à ceux en qui vous avez toute confiance. Tous les fournisseurs de messagerie électronique offrent la possibilité de créer plusieurs boîtes. Faites bien attention à ce que les deux adresses (privée et publique) ne comportent aucun point commun dans leur préfixe (caractères à gauche du @).



Le saviez-vous ?

La loi pour une république numérique a posé le principe de la portabilité des données. À partir de mai 2018, les prestataires de courriers électroniques seront tenus de permettre la migration des courriels et listes de contacts d'un utilisateur quand il souhaite changer d'opérateur.

Par exemple, si vous décidez d'utiliser Gmail au lieu de Yahoo, Yahoo devra vous permettre le transfert de vos e-mails et de vos contacts vers Gmail.

Le saviez-vous ?

En France, les internautes ont en moyenne 2 adresses e-mail mais 46% déclarent n'en avoir qu'une seule.

Source : Etude SNCD - EMA B2C, 2015

Contrôler le nom de l'émetteur des messages reçus

Soyez extrêmement prudent avec les messages dont l'origine vous est inconnue, dont le titre n'évoque rien de particulier pour vous et qui comporte des pièces jointes ou des adresses de site Internet. Au moindre doute, ne les ouvrez pas et effacez-les immédiatement. De même, si un de vos contacts vous explique, par e-mail, qu'il est en grande difficulté financière ou personnelle, et qu'il vous demande de l'argent soyez vigilant, car il peut s'agir d'un piratage.

Gardez aussi à l'esprit qu'un message vous demandant une réponse contenant des renseignements liés à votre vie privée, à vos coordonnées bancaires, vos divers identifiants et mots de passe ou à votre état civil est par définition suspect.

Si vous avez des doutes sur un courriel prétendant provenir d'une organisation légitime ou d'un contact habituel (banque, opérateur téléphonique, fournisseur électricité...), il vaut mieux vérifier auprès de cet organisme/personne l'authenticité du message.

Utiliser un logiciel antispam (logiciel de blocage de messages frauduleux)

Intégré à la plupart des logiciels de messagerie, parfois installé dans votre ordinateur, il est aussi proposé par votre fournisseur d'accès Internet. Ces logiciels sont en général paramétrables et vous permettent d'améliorer leur efficacité en choisissant les critères d'exclusion des messages reçus, par exemple : la provenance, un mot clé dans le titre, un mot clé dans le texte, etc.

Diversifier vos identifiants et mots de passe

Essayez de diversifier vos identifiants et mots de passe en évitant les évidences tels que : prénoms, région, département, nom du chien ou du chat, etc. Ce genre d'identifiant et mot de passe sont très faciles à retrouver pour un pirate chevronné.

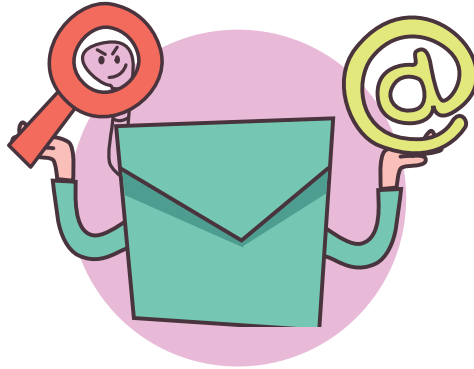
Le saviez-vous ?

En moyenne, 215 milliards de courriers électroniques ont été envoyés par jour dans le monde en 2015, hors les spams qui représentent entre 55 et 95 % du trafic total de l'e-mail.

Source : Radicati Group, mars 2016

Une entreprise de 100 personnes génère chaque année, avec son seul courrier électronique 13,6 tonnes d'équivalent CO₂, soit l'équivalent de 14 allers-retours Paris / New York.

Source : Analyses de Cycles de Vies des Technologies - Courriers électroniques, requête Web, clé USB : quels impacts environnementaux ?, ADEME, 7 juillet 2011



Signaler un mail illicite

Lorsque vous réceptionnez un e-mail de hameçonnage dont le contenu vous paraît frauduleux, n'hésitez pas à le signaler aux services de la police judiciaire. Pour se faire, deux options s'offrent à vous :

- Faites un copier/coller de son contenu et envoyez-le sur la plateforme « internet-signalement.gouv.fr »
- Remplissez le formulaire anonyme proposé par le site « pointdecontact.net » pour qu'il transmette votre signalement aux autorités compétentes (Point de Contact a été créé par l'Association des Fournisseurs d'Accès et de Services Internet qui regroupe les sociétés Orange, SFR, Bouygues Telecom, Google France, Microsoft France, Facebook France).

Pour en savoir plus : <http://www.afa-france.com>

Mémo



Pour éviter les messages indésirables ou dangereux :

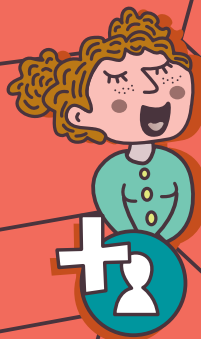
- 1** Utilisez deux adresses de messagerie : une privée à ne communiquer qu'à vos correspondants de confiance et une publique que vous utiliserez dans vos navigations sur le net (notamment pour vos achats).

-
- 2** Utilisez un logiciel antispam qui bloquera les messages frauduleux.

-
- 3** Diversifiez vos identifiants et mot de passe pour éviter le piratage de votre adresse mail.

Si vous recevez tout de même des messages frauduleux :

- 1** Signalez-les aux services de la police judiciaire via la plateforme « internet-signalement.gouv.fr » ou sur le site « pointdecontact.net ».



,les
réseaux
sociaux



Les réseaux sociaux

56 % des Français sont inscrits sur au moins un réseau social, et y passent en moyenne 1h16 par jour. Les utilisateurs ont généralement moins de 39 ans (80 à 90 % des 12-39 ans sont inscrits sur un réseau social), mais c'est une pratique qui tend à devenir intergénérationnelle puisque 40 % des 40-59 ans sont au moins inscrits sur un réseau social, mais aussi 10 % des 70 ans et plus (Arcep, étude sur les usages numériques en France, novembre 2015)

Le succès rencontré par les réseaux sociaux type Facebook, Twitter, Instagram, Snapchat, par les blogs et autres forums communautaires répond d'ailleurs à un besoin de lien social entre les internautes qui peuvent entre autres s'y divertir et rester en contact avec leurs proches, et « amis » plus ou moins éloignés. Les réseaux sociaux ont aussi pu influencer directement sur les grands bouleversements comme ceux du printemps arabe ou en servant de caisse de résonance aux actualités fortes (Fukushima, disparition de personnalités, attentats de Paris, etc.).

Toutefois, il ne faut pas oublier que ces pratiques, aussi ludiques ou influentes soient-elles, laissent des traces. En effet, les informations publiées sur sa page « personnelle » entrent dans l'espace public. Rien n'est donc jamais réellement privé sur Internet.

Les jeunes et les réseaux sociaux

- En France, 88% des 15-24 ans sont inscrits sur au moins un réseau social
- 76% des 15-24 ans sont sur Facebook
- 33% des 15-24 ans sont sur Snapchat
- 24% des 15-24 ans sont sur Twitter
- 18% des 15-24 ans sont sur Instagram

© Etude Médiamétrie : les 15-24 ans et le digital (novembre 2015)

1) Contrôlez les informations que vous diffusez

Il faut être particulièrement vigilant sur la nature des informations que l'on publie sur soi-même ou sur autrui. Par exemple, en 2015, trois adolescentes de 16 et 17 ans ont été mises en examen pour des violences verbales sur des personnes âgées, handicapées ou atteintes de la maladie d'Alzheimer. En stage dans une maison de retraite, les jeunes filles avaient posté 33 vidéos des violences sur l'application Snapchat.

En publiant des textes, des photos ou des vidéos, ou en les partageant, l'internaute devient un acteur à part entière dans la production de données sur le net. Il est donc entièrement responsable des informations qu'il diffuse ou relaie.

C'est pourquoi, il est important de réfléchir à ce que vous postez. En effet, vous n'êtes pas autorisé à tout faire sur la toile, et vous pouvez même risquer des sanctions judiciaires. Il faut donc se poser les bonnes questions avant de publier.

La barrière de l'écran peut, il est vrai, donner à certains l'illusion d'une certaine « impunité », qui peut virer, s'ils ne se contrôlent pas, à certains comportements répréhensibles (insultes à caractère antisémite, xénophobe, homophobe ou raciste, dénonciation calomnieuse, harcèlement...). Ainsi, l'auteur de l'infraction encourt jusqu'à 5 ans de prison et 45 000 euros d'amende lorsqu'il tient des propos injurieux ou mensongers (article 226-10 du Code pénal).

Le « cyber ami »

La notion « d'ami » n'a pas toujours la même signification sur Internet que dans la vie réelle. Les relations sont en effet dépersonnalisées, puisque vous ne voyez pas les réactions de l'autre. C'est pourquoi, il est important de bien réfléchir avant d'accepter un « ami » sur un réseau social. Pouvez-vous lui faire confiance ? Lui avez-vous déjà parlé en dehors d'Internet ?

2) Respecter la vie privée d'autrui

Quand vous publiez une photo ou une vidéo de vos amis, il est important d'avoir au préalable leur accord pour le diffuser sur Internet. Certes, ces moments peuvent vous sembler amusants, voire importants, mais cela peut parfois s'avérer gênant pour leurs vies personnelles et/ou professionnelles.

L'article 9 du code civil, dispose que « chacun a droit au respect de sa vie privée ». Une personne qui capte, enregistre ou transmet des paroles prononcées à titre privé ou capte l'image d'une personne sans son consentement encourt un an de prison et 45 000 euros d'amende (article 226-1 du code pénal). Et les tribunaux n'hésitent pas à sanctionner sévèrement les personnes qui tiennent des propos diffamatoires et des insultes à l'encontre d'autrui. Dans cette hypothèse, la victime pourra obtenir de lourds dommages et intérêts.

Par exemple, la cour d'Appel de Versailles, dans un arrêt daté du 8 juin 2000 (S.A. Multmania Production c/ Madame Lynda L., France Cybermédia, SPPI, Esterel), a condamné plusieurs sites Internet qui avaient diffusé des photographies d'une personne sans son accord, à lui verser la somme totale de 33 538 euros.

Les actes répréhensibles

■ Le cyberharcèlement

Une personne victime de cyberharcèlement peut recevoir un cumul de messages anonymes provenant de différentes sources, sur différents médias, tels son téléphone mobile, sa messagerie électronique, sa page personnelle sur un réseau social...

Ces messages menaçants et insultants peuvent prendre la forme d'intimidation ou chantage et sont parfois commis également à l'école, dans un club... Il arrive que les auteurs de ces messages demandent de l'argent pour que cesse la situation, exigent une rencontre ou la communication d'informations privées.

L'agresseur ne voit pas les réactions de souffrance de sa victime, ce qui annihile le sentiment de compassion et d'empathie car l'agresseur est derrière son écran et non face à la victime. La dépersonnalisation atteint non seulement la victime mais ses persécuteurs, qui ont tôt fait de se déresponsabiliser de leurs actes « virtuels ».

La victime de ce type de procédé montre des signes de repli sur soi, d'angoisse face à l'écran et de peur d'aller dans les lieux publics. C'est pourquoi, il ne faut pas hésiter à en parler autour de soi, pour d'une part, inciter son entourage à ne pas participer à ce genre de pratique et, d'autre part, donner à la victime quelques conseils utiles pour se défendre à savoir :

- Ne donner ses coordonnées personnelles qu'à des personnes de confiance
- Encourager la victime à parler
- L'inviter à ne pas répondre aux messages de ses harceleurs, tout en les conservant
- Prévenir le responsable des sites où ont lieu ces agissements, pour qu'ils en effacent le contenu. Les modérateurs des réseaux sociaux ne pourront jamais tout surveiller.



Dans l'exemple des stagiaires qui filmaient sur Snapchat des actes de maltraitance envers des personnes âgées, ce sont des camarades de classe, qui après avoir visionné les scènes, ont prévenu leurs enseignants.

Dans les cas les plus graves, ne pas hésiter à porter plainte à la police ou la gendarmerie, et leur communiquer la copie des messages tendancieux. En effet, le cyberharcèlement est passible de deux ans d'emprisonnement et de 30 000 € d'amende (article 222-33-2 du code pénal).

Un numéro vert national a été mis en place, **Net Ecoute (0800 200 000)** géré par l'association e-Enfance. Des informations techniques juridiques et psychologiques adaptées à la victime de cyberharcèlement, à sa famille et au personnel éducatif peuvent être proposées. Par ce canal, il est parfois possible, de faire cesser les manifestations en ligne du harcèlement.

■ **L'usurpation d'identité :**

L'usurpation d'identité, est le fait de prendre délibérément l'identité d'une autre personne vivante, généralement dans le but de réaliser des actions frauduleuses commerciales, civiles ou pénales, comme régulariser sa situation au regard de l'émigration, accéder aux finances de la personne usurpée, ou de commettre en son nom un délit ou un crime, ou d'accéder à des droits de façon indue.

Cette infraction est punie d'un an d'emprisonnement et de 15 000 € d'amende (article 226-4 du code pénal). Elle est applicable notamment lorsqu'une personne utilise votre identité sur les réseaux sociaux pour diffuser des informations erronées. Attention, cette infraction nécessite un dépôt de plainte au commissariat ou à la gendarmerie de votre lieu de domicile.

■ **L'incitation à la violence, au suicide, à l'apologie de crimes contre l'humanité à la discrimination ou à la haine raciale :**

En droit français, l'incitation à la violence, à la discrimination ou à la haine raciale est un délit³ dont l'auteur peut encourir jusqu'à cinq ans d'emprisonnement et 45 000 euros d'amende. Si vous constatez qu'un blog, une vidéo ou l'article d'un site internet a pour contenu des écrits, des discours portant provocation et/ou apologie de délits ou crimes contre les personnes ; sont racistes ou discriminatoires, et ce à raison de l'origine, la religion, l'appartenance ou non à une ethnie, à raison de son sexe, son orientation sexuelle ou de son handicap, n'hésitez pas à contacter le site de l'hébergeur, pour qu'il procède à son retrait.

Dans les cas les plus graves, portez plainte à la police ou la gendarmerie, en leur communiquant la copie des messages injurieux ou à caractère raciste...

³ délit : acte ou comportement contraire à la loi jugé par le tribunal correctionnel



Vous pouvez aussi :

- Faire un copier/coller du contenu puis l'envoyer sur la plateforme « internet-signalement.gouv.fr
- Remplir le formulaire anonyme proposé par le site « pointdecontact.net », pour qu'il transmette le signalement aux autorités compétentes.

3) Quelques conseils utiles pour bien utiliser ces services

Paramétrer correctement son profil

Quel que soit le site sur lequel vous vous créez un compte, il est important de prendre le temps de paramétrer correctement votre profil. Ne faites jamais confiance a priori sur les choix de « paramétrage par défaut » du site hébergeur, car il est fréquent de tomber sur de mauvaises surprises. En effet, ce que recherche avant tout un hébergeur, c'est d'augmenter au maximum le nombre de visites du site ou du service.

Rester si possible anonyme

Quand vous le pouvez, et surtout sur des forums communautaires, blogs, messagerie instantanée, créez un **pseudonyme**. En effet, mieux vaut ne pas trop se dévoiler auprès de personnes que l'on connaît peu. Il est facile d'identifier une personne sur Internet si elle donne beaucoup d'informations la concernant. Or, qui aimerait que son (futur) employeur trouve une photo compromettante prise lors d'une soirée entre amis, en faisant une simple recherche sur Internet ?

Le saviez-vous ?

Le droit à l'oubli pour les mineurs

Les jeunes, ultra-connectés, n'ont pas toujours conscience des risques auxquels ils s'exposent. Ils peuvent faire effacer leurs données personnelles grâce à une procédure accélérée spécifique. Grâce à la loi pour une République numérique, en cas de difficulté à obtenir l'effacement de données publiées par une personne, il est possible de saisir la CNIL qui statuera dans un délai de 15 jours.

Le saviez-vous ?

Des mesures pour les données après le décès

Depuis mars 2017, la loi permet également aux internautes de prendre des dispositions concernant l'utilisation de leurs comptes sur les services Internet après leur mort, ainsi que le devenir de leurs données personnelles. Un héritier de ses données personnelles pourra être désigné, afin qu'il puisse y accéder et supprimer les comptes du défunt sur les réseaux sociaux.

Ne pas hésiter à se « googliser »

Cette méthode consiste à lancer une recherche sur les principaux moteurs (Google, Bing, Yahoo, etc.) avec votre nom et prénom et à consulter les résultats. Le site « 123people.com » est également un bon moyen pour détecter les informations publiques associées à votre nom, qui circulent sur la toile.

Ainsi, si vous constatez des informations fausses ou compromettantes, il vous suffira de vous rapprocher de l'éditeur de cette donnée pour en obtenir l'effacement.

Se connecter en mode sécurisé

De même, certains réseaux sociaux offrent la possibilité de se connecter sur leur site en mode sécurisé. Pour ce faire, il faut vous identifier dans l'onglet sécurité des paramètres de votre compte, et choisir l'option requise. Désormais, vous aurez la possibilité de surfer via une adresse commençant par « https:// », et non seulement en « http:// », ce qui limite les risques d'hameçonnage ou « phishing »².

² L'hameçonnage, ou « phishing », consiste en l'envoi d'un courriel qui prétend être d'une entreprise légitime ou d'une administration, vous demandant de visiter un site web et d'y saisir des informations personnelles qui seront captées et exploitées de façon malveillante par les fraudeurs.

Mémo

Pour une bonne utilisation des réseaux sociaux, blogs, messageries instantanées et forums :

- 1 Faites preuve de vigilance concernant les informations que vous publiez sur vous-même ou sur autrui, car votre responsabilité peut être engagée.
- 2 L'usurpation d'identité, la discrimination ou l'incitation à la haine raciale sont lourdement sanctionnées. N'hésitez pas à signaler ces pratiques auprès d'un adulte, l'hébergeur du site ou la police/gendarmerie dans les cas les plus graves.
- 3 Paramétrez correctement votre profil, et ne faites jamais confiance a priori sur les choix de « paramétrage par défaut » du site hébergeur.
- 4 Quand vous le pouvez, et surtout sur des forums communautaires, blogs ou tchat, créez-vous un pseudonyme.
- 5 N'hésitez pas à lancer une recherche sur les principaux moteurs (Google, Bing, Yahoo, etc.) avec votre nom et prénom puis consultez les résultats pour détecter les informations publiques associées à votre nom, qui circulent sur la toile.
- 6 Quand cela est possible, connectez-vous en mode sécurisé sur ces sites (adresse commençant par « https:// »), afin d'éviter les risques d'hameçonnage.

Le telech[icône]n- gement



Le téléchargement

Si aujourd'hui le téléchargement a pris une signification péjorative, car trop souvent associé à « l'illégalité », il ne faut pas oublier que le téléchargement est indissociable de l'utilisation d'Internet. En effet, cette opération consiste à copier des fichiers accessibles via votre liaison Internet et à les mettre sur votre ordinateur, afin de permettre l'échange de données numériques à distance. Il comprend notamment les fichiers reçus en pièce jointe du courrier électronique.

1) Les différents types de fichiers téléchargeables

La nature de ces fichiers est extrêmement diverse. On peut les classer dans deux grandes familles :

- les fichiers passifs qui ont vocation à être lus et éventuellement modifiés : textes, photos, vidéos, sons, musiques...
- les fichiers actifs qui contiennent des programmes exécutables : mises à jour et autres programmes de toutes sortes...

ATTENTION

Un fichier, quelle que soit sa nature, peut en cacher un ou plusieurs autres. C'est le cas notamment des virus⁶ conçus pour endommager ou pour espionner votre ordinateur. Ces fichiers infectés peuvent être neutralisés au moyen d'un programme antivirus qu'il faut donc impérativement installer et régulièrement mettre à jour. Notez qu'actuellement la grande majorité des programmes antivirus comporte un système automatique de mise à jour.

⁶ Le terme « virus » est de plus en plus utilisé de manière générique et recouvre tous les types de logiciels introduits à votre insu dans votre ordinateur, ayant un effet néfaste à son fonctionnement ou visant à s'introduire dans votre vie privée. Il est donc plus simple de considérer que ce terme de virus englobe les « virus ou malware », « espions ou spyware », « marionnettiste ou bot », « arnaqueur ou rogue ». Les remèdes existent : ce sont les programmes antivirus, en général adaptés à tous ces types de virus.

2) Et les applications dans tout ça ?

Une application mobile est un programme téléchargeable de façon gratuite ou payante et exécutable à partir du système d'exploitation d'un smartphone, d'une tablette ou une montre connectée... Les applications visaient d'abord à faciliter la récupération d'informations telles que le courrier électronique, calendrier électronique, contacts, météo. Face au succès rencontré, les applications ont connu une expansion rapide dans d'autres domaines comme les jeux mobiles, les applications bancaires, les réseaux sociaux, etc. A noter que de nombreuses applications se développent en lien avec un objet connecté, car un objet connecté n'a de sens que s'il est associé à une application qui restitue les données transmises.

Le saviez-vous ?

Selon Médiamatrive, début 2016, les utilisateurs de smartphones avaient en moyenne 28 applications mobiles installées sur leur téléphone.

Bon à savoir

les objets connectés

Grâce au développement des technologies de l'information et des communications, des milliards d'objets et services dans le monde sont aujourd'hui connectés. Ils sont présents dans les domaines de la santé, de la sécurité, de l'énergie, de la domotique....

D'où viennent-ils ?

Tout a commencé par le développement de la technologie RFID (Radio Frequency identification). Il s'agit en réalité d'un montage électronique miniature introduit dans ou sur un objet et capable de stocker, d'envoyer et de recevoir des informations concernant cet objet. Très rapidement les ingénieurs ont développé des applications telles que des systèmes antivol, ou encore des clés électroniques. Chaque objet est devenu identifiable, localisable, et suivi en temps réel. Cette réussite technologique s'est transformée en succès commercial. Ainsi, on prévoit 50 milliards d'objets connectés dans le monde dans les trois prochaines années.

Que sont-ils ?

En réalité, il n'existe pas de définition officielle de l'objet connecté. Du point de vue technique, un objet connecté est un objet auquel un dispositif électronique a été greffé et qui le rend capable de capter, de stocker, d'envoyer, de recevoir et même d'analyser des informations sur l'objet en question et ou sur son environnement immédiat. Du point de vue opérationnel, un objet connecté peut communiquer avec un smartphone, et/ou avec un autre objet connecté, et/ou directement se connecter à Internet en vue d'exploiter les données qu'il contient. Un objet connecté est donc un objet qui prévoit la collecte et l'utilisation de données par une connexion assurée par l'objet lui-même.

Où les trouve-t-on ?

Par exemple, dans le domaine automobile, une marque européenne a développé une application qui permet de garer sa voiture de l'extérieur en pianotant sur son smartphone. Dans le domaine médical, plusieurs modèles de tensiomètres connectés sont disponibles et permettent au patient de partager ses données de tension artérielle avec son médecin traitant. Autre exemple, des lentilles connectées dotées d'un capteur qui mesure le taux de sucre dans la larme du patient diabétique seront bientôt mises sur le marché.

Certains de ces objets nous rendent la vie plus facile, c'est le cas par exemple des dispositifs embarqués dans les voitures qui évitent les fausses manœuvres ou les obstacles, ou préviennent les secours automatiquement en cas d'accident (eCall).

ATTENTION

Les consommateurs doivent rester attentifs à l'usage qu'ils ont de ces technologies.

Nos conseils

- Vérifiez toujours dans les conditions générales, dans la notice, comment sont collectées vos données personnelles, pour quelle durée et quelle utilisation.
- Un objet est susceptible d'être partagé par plusieurs utilisateurs y compris au sein d'une même famille. Veillez à ce que le paramétrage par défaut limite à chaque utilisateur l'accès en propre et à lui seul aux données qui le concernent. La connexion doit être non activée par défaut, tant en usage local qu'en usage partagé.
- Vous devez pouvoir effacer l'historique de vos données personnelles, notamment en cas de vente, ou lors de la fin de vie du produit.
- N'hésitez pas à vérifier si le professionnel indique la consommation d'énergie de l'objet connecté, son rayonnement électromagnétique, voire sa réparabilité.

3) Quelques conseils utiles avant de télécharger

Installer un logiciel antivirus

Avant de vous engager dans le téléchargement, installez un logiciel antivirus sur votre ordinateur.

Les programmes antivirus sont très nombreux sur le marché et leurs distributeurs redoublent d'imagination pour vous convaincre qu'ils proposent le remède parfait. Or, ni le remède parfait ni la protection sans faille n'existent dans le domaine informatique. Le choix est donc difficile d'autant plus que l'étendue des offres et des prix proposés sont surprenants. Il existe aussi des antivirus gratuits tout à fait valables. Enfin, la plupart des fournisseurs d'accès Internet proposent des solutions de protection moyennant quelques euros supplémentaires sur votre abonnement qui, au bout de quelques mois ou quelques années, peuvent s'avérer très onéreuses.

Avant de le choisir n'hésitez pas à vous informer, soit auprès de votre fournisseur d'accès, soit en consultant la presse de vulgarisation qui édite régulièrement des numéros hors-série sur le sujet, pratiques et bien documentés.

Bon à savoir

Le **streaming** permet la lecture de fichiers multimédia comme par exemple écouter de la musique ou regarder des vidéos avec votre ordinateur personnel. Contrairement au téléchargement, qui nécessite de récupérer l'ensemble des données d'un morceau ou d'un extrait vidéo avant de pouvoir l'écouter ou le regarder, ce protocole permet de lire directement un flux de données au fur et à mesure de son arrivée sur votre ordinateur. L'avantage du streaming est qu'il vous évite d'encombrer le disque dur de votre ordinateur avec des fichiers multimédia en général très volumineux.

Le streaming : payant ou gratuit ? Légal ou illégal ?

L'internaute qui met en ligne des œuvres sans autorisation en téléchargement ou streaming commet un délit de contrefaçon, passible d'une peine de 3 ans de prison et 300 000 € d'amende. Le spectateur peut même être considéré comme receleur.

Être attentif à la valeur marchande des fichiers

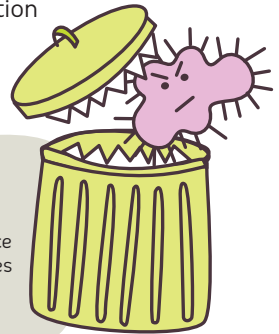
Vous devez être attentif à la valeur marchande des fichiers que vous téléchargez. En effet, si le téléchargement de certains fichiers est gratuit, pour d'autres, le téléchargement est payant car soumis aux règles de la propriété intellectuelle.

Un fichier, comme tout autre produit, peut donc faire l'objet de contrefaçon, de piratage, de vente et de distribution illicite. Gardez à l'esprit que lorsque vous téléchargez un fichier piraté ou dont l'origine n'est pas clairement identifiée, vous pouvez vous trouver dans la même situation que lorsque vous achetez une montre contrefaite sur un marché. La contrefaçon est un délit pour lequel l'acheteur peut encourir jusqu'à trois ans d'emprisonnement et 300 000 euros d'amende.

Enfin, il existe sur Internet de nombreux sites de téléchargement, parfaitement légaux, vous proposant des fichiers gratuits. Ils sont généralement financés par la publicité, la promotion commerciale et l'appel aux dons.

Bon à savoir

De nombreux fournisseurs d'accès proposent un service légal et payant de téléchargement d'œuvres artistiques numérisées à des prix souvent très intéressants.



Vérifier le statut du site hébergeur

Avant de télécharger un fichier, vérifiez l'origine et le statut du site qui propose le téléchargement. Là aussi, il n'y a pas de recette infallible pour échapper aux propositions illégales et il faut souvent se référer au dicton : « c'est trop beau pour être vrai ! ». Il en va de même dans le cas des fichiers contenant des œuvres artistiques numérisées (musique, films, livres) dont la copie, la distribution et même la fabrication sont très faciles à mettre en œuvre. Comment protéger d'une part les producteurs et les auteurs ainsi dépossédés d'une partie de leurs revenus potentiels et d'autre part les consommateurs de bonne foi qui n'ont pas toujours les moyens et les connaissances pour éviter ces pièges ?

Pour faire face à ce type de contrefaçon particulière, la France, a mis en place la HADOPI (Haute autorité pour la diffusion des œuvres et la protection sur Internet). Son rôle est de promouvoir le développement de l'offre légale, d'observer l'utilisation licite et illicite des œuvres sur Internet, de protéger les œuvres à l'égard des atteintes aux droits qui leur sont attachés et de réguler l'usage des mesures techniques de protection. Pour protéger les droits d'auteur la HADOPI a mis en place un dispositif de protection aussi appelé « la riposte graduée ». Ce dispositif consiste à identifier les contrevenants, à les informer qu'ils sont en situation illicite et à leur indiquer les peines encourues. En cas de récidive, les peines appliquées sont graduelles et peuvent aller jusqu'à une amende de 1 500 euros.

4) Vous avez dit cloud ?

L'appellation « cloud » (« nuage » en anglais) désigne l'externalisation de vos données sur des serveurs distants, ce qui évite notamment d'avoir à stocker ces dernières sur un seul ordinateur/tablette/smartphone.

L'intérêt est d'accéder à ses données depuis n'importe quel ordinateur connecté à Internet et de les synchroniser sur plusieurs appareils. Les bénéfices sont multiples : gain d'espace, de ressources, de temps et d'argent. L'utilisateur peut accéder librement à ses documents sans se soucier de la machine qu'il utilise.

Pour le consommateur, le cloud lui sert surtout pour :

- la sauvegarde, le stockage et le partage des données, principalement des photos,
- la délocalisation des outils comme le traitement de texte,
- les coffres-forts électroniques pour le stockage protégé des documents sensibles (copies de cartes d'identité, etc.)

Pour illustrer facilement l'intérêt du cloud, imaginez la scène suivante : vous êtes étudiant et rédigez les premières pages d'un rapport à partir d'un logiciel de traitement de texte présent sur votre poste. Il vous suffit de déporter votre travail sur le cloud et de vous connecter sur ce dernier à partir de votre ordinateur personnel afin de poursuivre tranquillement votre rapport, sans avoir à installer le logiciel en question. Surtout, vous pouvez y accéder à tout moment, même depuis un autre ordinateur, simplement en vous identifiant auprès de l'hébergeur de vos données.

Les clouds les plus utilisés sont i-cloud d'Apple, DropBox ou Gmail par Google.

Mais attention l'utilisation du cloud n'est pas sans risques, car qui dit Cloud dit web, et donc une sécurité limitée. Dès lors qu'une donnée personnelle se trouve sur un serveur distant, il existera toujours un risque qu'elle soit interceptée à un moment donné (Rappelez-vous du piratage des photos intimes dévoilées de chanteuses et actrices américaines stockées sur un cloud, dont un hacker avait récupéré les mots de passe).

Si la société propriétaire des serveurs de stockage est tenue de proposer une sécurisation optimale de ses serveurs, l'internaute a aussi un rôle important dans la sécurisation de ses données.

Pour protéger efficacement votre compte « cloud » :

- Utilisez un mot de passe complexe composé de majuscules et de minuscules et contenant un ou plusieurs caractères spéciaux. Par exemple **Xjuv273p)<**
- Privilégiez la question de sécurité dont vous êtes le/la seul(e) à connaître la réponse (famille et amis exclus).
- Enfin, privilégiez les clouds qui proposent **l'identification en deux temps**, une pratique quasi inviolable puisqu'après avoir décliné vos identifiants et mots de passe, un code à quatre chiffres est envoyé sous forme de sms.

Mémo

- 1 Le téléchargement est indissociable de l'utilisation d'Internet.
- 2 Il y a deux grandes familles de fichiers téléchargeables : les fichiers passifs (textes, photos, vidéos, sons, musiques...) et les fichiers actifs qui contiennent des programmes exécutables (mises à jour...).
- 3 Avant de vous engager dans le téléchargement :
 - installer un logiciel antivirus sur votre ordinateur
 - vérifier l'origine et le statut du site qui propose le téléchargement pour échapper aux propositions illégales
- 4 Le cloud consiste à l'externalisation de vos données sur des serveurs distants, ce qui permet d'y accéder depuis n'importe quel ordinateur connecté à Internet et de les synchroniser sur plusieurs appareils.
- 5 Avant d'ouvrir un compte « cloud » :
 - utilisez un mot de passe complexe composé de majuscules/minuscules et caractères spéciaux.
 - attention : opter pour la question de sécurité dont vous êtes le seul à connaître la réponse.



l'achat
en
ligne

L'achat en ligne

Internet est devenu un mode d'achat incontournable pour les internautes. Ainsi, 36,6 millions de Français ont acheté en ligne en 2016, soit 82,7% des internautes⁸. Toutefois, il convient de rester vigilant car Internet est une galerie marchande mondiale où les règles ne sont pas partout les mêmes. Voici donc quelques astuces pour acheter en toute connaissance de cause sur le net.

1) L'achat entre particuliers sur les plateformes de vente

En cas d'achat

L'achat et la vente sur des plateformes, comme eBay ou le Bon coin, rencontrent un réel succès auprès des particuliers, qui peuvent vendre ou revendre des objets dont ils n'ont plus l'utilité, et acheter des produits à moindre frais, mais aussi louer un véhicule ou un logement pour les vacances, tenter le covoiturage, etc.

Mais attention, les règles et les garanties applicables lors de l'achat du produit ne sont pas les mêmes, si vous achetez auprès d'un particulier ou d'un professionnel. Ainsi, si la vente s'effectue entre un particulier et un professionnel, le délai de rétractation s'applique. En revanche, si la vente s'effectue entre deux particuliers, le délai de rétractation ne s'applique pas. Mais vous pourrez toujours exiger du vendeur particulier le remboursement ou l'échange du produit, si le produit n'est pas livré ou présente un défaut non mentionné dans l'annonce qu'il a rédigé.

⁸ FEVAD, chiffres clés de la vente à distance e-commerce, édition 2017

En cas de vente

■ Bien rédiger l'annonce

En tant que particulier, si vous passez une annonce sur une plateforme, il est important de préciser dans l'annonce les caractéristiques du produit, et ses défauts éventuels, car vous êtes responsable de la bonne exécution du contrat.

■ Envoi de la commande en suivi

Lors de l'envoi de la commande, il est préférable d'opter pour un suivi d'expédition, car si le colis se perd, votre responsabilité peut, là encore, être engagée, et vous serez contraint de rembourser l'acheteur.

Le rôle de la plateforme numérique collaborative

En cas de problème à la suite d'un achat sur une plateforme collaborative, vous devez en principe vous adresser directement au vendeur, car c'est avec lui que vous avez contracté et non la plateforme. Certaines plateformes jouent néanmoins le rôle d'intermédiaire dans le règlement des litiges. D'autres encore ont noué des partenariats avec des sociétés d'assurance, et proposent ainsi des garanties lors de certains événements (garantie casse ou vol par exemple). Avant toute rédaction d'annonce ou avant un achat, n'hésitez pas à consulter leurs conditions générales, afin de connaître les règles de fonctionnement de différente(s) plateforme(s) concurrente(s).



2) L'achat sur un site marchand

Vérifier la fiabilité du site

Internet est une galerie marchande mondiale. Il est donc possible d'acheter partout dans le monde. Toutefois, pour éviter les ennuis, voici quelques conseils utiles :

- **Le commerçant est clairement identifié** : ses coordonnées postales, électroniques et téléphoniques apparaissent de façon claires.

Bon à savoir

Ces informations peuvent se trouver dans la partie « qui sommes nous ? », « contact » ou « informations légales » du site.

- **Le site est situé dans l'Union européenne** : les Etats membres de l'Union européenne ont tous adopté des règles protectrices pour le consommateur. En général, elles sont assez similaires au droit français.
- **Les conditions générales de vente sont accessibles**, et les paragraphes relatifs aux délais de livraison, aux garanties commerciales et aux conditions d'annulation sont clairs.
- **S'informer sur la réputation du site marchand** : par une simple requête dans un moteur de recherche, vous pourrez savoir si le commerçant fait l'objet d'évaluations positives par des internautes sur des sites et forums communautaires.
- **Rechercher si le site est en liquidation judiciaire** : pour les sociétés établies en France, vous pourrez trouver cette information sur les sites bodacc.fr, infogreffe.fr ou société.com, à partir de la dénomination sociale du professionnel ou son numéro RCS (Registre du commerce et des sociétés).

La commande en ligne

▪ Etape 1 : la sélection du produit ou service

Avant toute commande, le professionnel doit détailler les caractéristiques du produit ou du service qu'il vend, afin de vous permettre d'évaluer sa qualité.

Par exemple, lors de l'achat d'un ordinateur, il doit vous être indiqué la taille de l'écran, la capacité de la mémoire vive et du disque dur, mais aussi les accessoires fournis comme une webcam, une souris...

Le cyber-marchand doit aussi vous informer du prix du produit ou service, et des prestations supplémentaires qu'il propose, comme les frais de livraison ou de mise en service.

Une fois que vous avez sélectionné le (les) produit(s) ou service(s) désiré(s), vous le(s) retrouvez dans la rubrique « panier » ou « commande ».

▪ Etape 2 : le premier clic = le détail de la commande

Le premier clic doit vous permettre de vérifier le détail de la commande et son prix, mais aussi de corriger les éventuelles erreurs (notamment sur vos coordonnées, la double commande...).

▪ Etape 3 : le deuxième clic = la validation de la commande

En général, une nouvelle fenêtre apparaît, qui récapitule le détail de la commande et le montant total à payer. Une fois que vous validez cette étape, **vous exprimez par ce « double clic » votre accord au contrat, ce qui équivaut à votre signature.**

Une fois validée, le site marchand doit vous adresser un accusé de réception récapitulant le détail de la commande, accompagnée d'un formulaire type de rétractation, sur votre boîte mail personnelle. Ce mail vous garantit que la commande a bien été enregistrée.

Le saviez-vous ?

Attention aux faux avis en ligne !

88 % des internautes consultent les avis sur les plateformes consommateurs avant d'acheter (sondage IFOP décembre 2014). Néanmoins la fiabilité des avis en ligne n'est pas toujours assurée. N'hésitez pas à consulter plusieurs sites/forums pour vous renseigner sur la réputation du site ou du produit souhaité.

Depuis 2013, il existe une norme AFNOR NF Z74-501 relative au traitement des avis des consommateurs en ligne, mais elle est seulement d'application volontaire pour les entreprises. La loi pour une République numérique, va plus loin car son article 15 impose aux plateformes Web qui diffusent des avis de consommateurs d'indiquer explicitement si les publications ont été vérifiées. Un décret viendra préciser les conditions d'application de cette nouvelle règle.

Conserver sur support durable l'ensemble des éléments de la vente.

Conservez toujours par précaution ce mail, les coordonnées de l'entreprise, la fiche descriptive du produit et les conditions générales de vente, car en cas de problème, vous pourrez vous servir de ces éléments.

Bon à savoir

Le délai de rétractation

Si le produit commandé ne vous convient pas, vous avez un délai de 14 jours à compter de sa réception pour changer d'avis, il s'agit du droit de rétractation. Attention, pour les prestations de service, le délai de 14 jours court à compter de la validation de la commande. Vous n'avez pas à expliquer les raisons de votre décision. En pratique, mieux vaut envoyer un courrier ou le formulaire type de rétractation en recommandé avec accusé de réception. Ensuite, il vous faudra renvoyer le produit à vos frais, dans les 14 jours suivant l'envoi de votre décision de rétractation. Le professionnel dispose alors de 14 jours pour vous rembourser, mais peut différer le remboursement jusqu'à réception de votre produit retourné.

ATTENTION

la vente est ferme et définitive, c'est-à-dire que le droit de rétractation ne s'applique pas lors de l'achat des produits suivants :

- les journaux, périodiques, magazines
- les CD, DVD
- les services de pari ou de loteries autorisées
- l'hébergement
- le transport
- la restauration
- les prestations de loisirs, les achats de voyage à forfait et de billets de spectacle
- les denrées alimentaires
- tout bien acheté à un particulier

Le paiement en ligne

Le paiement en ligne est encore aujourd'hui une source de stress pour le consommateur. Les possibilités d'usurpation des données bancaires, en particulier des cartes bancaires, ne sont pas négligeables. Néanmoins, les transactions protégées sont performantes et les recours sont possibles.

Les problèmes rencontrés par les consommateurs effectuant des achats sur Internet relèvent parfois plus du manque d'expérience et de l'étourderie. Quelques bons réflexes et de bonnes habitudes vous permettront de réaliser vos achats en réduisant significativement les risques.

Avant d'engager des achats sur Internet, vérifier que vous êtes bien sur un site protégé

Au moment de la commande, l'adresse indiquée dans la barre d'adresse de votre navigateur doit commencer par le préfixe **https** (*mode de cryptage des données personnelles : nom, adresse, coordonnées bancaires*). De plus, l'**icône d'un cadenas fermé** doit apparaître soit à droite de la barre d'adresse soit dans la barre d'état, en bas à droite de la fenêtre du navigateur. Si vous cliquez sur cette icône, vous accéderez aux informations de sécurisation du site.

ATTENTION

le cadenas garantit seulement la sécurisation des communications entre vous et le serveur. Il ne garantit pas la fiabilité du site ou l'honnêteté du marchand.



Cette première vérification faite, il faut ensuite choisir parmi les modes de paiement proposés par le site de vente en ligne et qui peuvent être :

- La carte bancaire
- Le chèque bancaire
- Le paiement à réception de la commande
- Le paiement via un site de paiement en ligne
- L'e-carte bancaire
- Le virement bancaire

Les sites marchands en ligne doivent proposer au minimum deux méthodes de paiement en ligne distinctes. Dans leur grande majorité les sites marchands donnent la préférence au paiement par carte bancaire et au paiement via un site de paiement en ligne (PayPal, Google Wallet...).

La carte bancaire

Le paiement par carte bancaire est le plus utilisé car extrêmement simple à mettre en œuvre, tant pour le vendeur que pour le consommateur. Une fois les données bancaires entrées et validées (numéro visuel de carte à 16 chiffres, date de fin de validité à 4 chiffres et les 3 derniers chiffres du pictogramme au dos de la carte), la transaction est conclue et votre carte bancaire est donc engagée pour la somme inscrite sur le bon de commande.

Bon à savoir

la sécurisation de la transaction par 3D Secure

Lors du paiement par carte bancaire, certains sites Internet pourront vous demander un code supplémentaire fourni par votre banque, avant de valider votre achat. Il s'agit du système 3D Secure qui permet de s'assurer que la carte bancaire servant au paiement de la commande est bien la vôtre. En pratique, votre banque vous enverra un code par SMS ou vous demandera de répondre à une question secrète.

Faire un suivi rapproché du débit de votre carte bancaire

Une fois la confirmation de commande réceptionnée sur votre adresse de messagerie, faites ensuite un suivi rapproché du débit de votre carte bancaire en consultant votre relevé de compte. Au moindre doute, contactez le site de vente en ligne et/ou votre banque.

Les 4 piliers de sécurité pour le paiement par mobile ou tablette

1

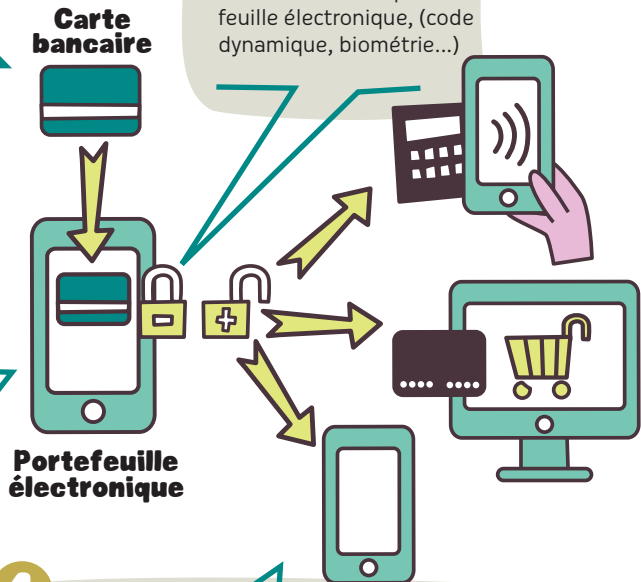
La banque contrôle l'identité du porteur de la carte, lorsqu'il veut inclure une carte bancaire dans un portefeuille électronique

2

Un numéro virtuel (token) propre à chaque support (téléphone, tablette) sera donné par le système de paiement, pour les transactions (et non vos coordonnées de carte bancaire)

3

Authentification sécurisée du porteur lors de l'utilisation du portefeuille électronique, (code dynamique, biométrie...)



4

Avant la **validation définitive** de l'achat, une nouvelle validation est demandée au consommateur via un support distinct (code via sms, e-mail, empreinte digitale...)

Le chèque bancaire

Cette méthode, de moins en moins proposée sur les sites marchands, est en voie de disparition. Son principal désavantage pour le consommateur est le délai de livraison car le vendeur en ligne ne déclenchera la procédure de livraison qu'après réception et encaissement du chèque. Si vous utilisez ce mode de paiement, les conseils donnés pour le paiement par carte bancaire s'appliquent aussi.

Paie ment à réception de la commande

Le paiement à réception de la commande est, bien entendu, le moins risqué mais très peu utilisé par les sites marchands. Si ce mode de paiement vous est proposé, choisissez-le ! Néanmoins, gardez toujours une copie de la commande en ligne ou du message de confirmation.

Site de paiement en ligne

Cette méthode de paiement est certainement la plus populaire car elle a la même efficacité que le paiement par carte bancaire sans vous obliger à laisser vos coordonnées de carte bancaire sur le site marchand. Pour utiliser ce mode de paiement, il faut s'inscrire sur le site de paiement en ligne. Les deux sites les plus utilisés en France sont PayPal et Google Wallet.

La e-carte bancaire

Le but de la e-carte bancaire, comme pour les sites de paiement en ligne, est de vous éviter de laisser vos coordonnées de carte bancaire sur chaque site de vente en ligne que vous utilisez. Ce service est délivré par de nombreuses banques et il est en général payant. La e-carte bancaire nécessite en outre un petit logiciel à installer sur votre ordinateur qu'il faudra lancer à chaque fois que vous souhaitez faire des achats sur Internet en utilisant ce mode de paiement.

Vérifier que votre banque offre cette prestation

Si vous souhaitez utiliser la e-carte bancaire pour faire vos achats en ligne, contactez votre banque pour vérifier qu'elle fournit bien ce type de service. Demandez également à consulter les conditions d'utilisation. N'utilisez pas le paiement par e-carte bancaire pour les achats nécessitant la présentation de votre carte bancaire au moment de la réception ou du retrait (par exemple les billets de trains SNCF achetés sur Internet et retirés à une borne).

Le virement bancaire

Le virement bancaire est vraisemblablement le plus sûr des modes de paiement pour les achats sur Internet. La procédure est similaire au paiement par chèque puisque le site de vente en ligne ne validera la commande qu'après exécution et vérification dudit virement. Les sites de vente en ligne qui pratiquent ce mode de paiement vous communiquent donc, au moment du paiement, leur Relevé d'identité bancaire (RIB).

Vérifier le coût du virement facturé par votre banque

Si vous pratiquez le paiement par virement bancaire, il est préférable d'avoir accès à votre compte bancaire en ligne. Il est également fort conseillé de vérifier le coût facturé par votre banque pour ce type de transaction.



Tableau récapitulatif

Bien choisir son mode de paiement en ligne :

La carte bancaire :	▪ Le plus utilisé... Attention, restez vigilant !
Le chèque bancaire :	▪ En voie de disparition
Le paiement à réception de la commande	▪ Généralement rejeté par les sites de vente en ligne
Le paiement via un site de paiement en ligne	▪ Le plus populaire
La e-carte bancaire	▪ Un peu compliqué... Attention aux coûts !
Le virement bancaire	▪ Le plus sûr mais un peu lent

La livraison

Les délais de livraison

Lorsque vous achetez un bien ou un service en ligne, le cyber-vendeur est tenu de préciser sur son offre de vente les modalités de livraison de la commande (point relais, à domicile...).

En effet, il doit indiquer, avant la conclusion du contrat, la date limite de livraison du bien ou service. A défaut, la commande devra être livrée dès la conclusion du contrat.

En cas de litige lié à la livraison, plusieurs scénarios peuvent se présenter :

■ Absence de livraison

En cas d'absence de livraison, vous devez au préalable adresser au vendeur une mise en demeure de procéder à la livraison effective du bien dans un délai déterminé, par exemple 8 à 15 jours.

Faute de respecter ce délai supplémentaire, vous pouvez annuler la vente, par lettre recommandée avec avis de réception.

Le contrat est considéré comme rompu à réception par le professionnel de cette lettre recommandée sauf si dans l'intervalle, vous avez réceptionné la commande.

Dès lors, le cybervendeur est tenu de rembourser votre achat dans les 14 jours suivants la réception de votre demande d'annulation et de prendre en charge les éventuels frais de retour de celui-ci. Passé ce délai, la somme est majorée de 10% si le remboursement intervient au-delà de 30 jours, 20% au-delà de 60 jours et 50% au-delà de ce terme.

Cas particulier : **Votre commande a été expédiée mais vous ne l'avez pas reçue**

Dans tous les cas, il appartient au professionnel de rapporter la preuve de la réception de la commande. S'il ne peut pas prouver la livraison, il devra alors vous renvoyer le colis ou vous rembourser.

- **Livraison hors délai**

Malgré le retard de livraison, vous souhaitez encore maintenir votre commande. Vous devez écrire au professionnel, par courrier recommandé, pour le mettre en demeure d'exécuter son obligation dans un délai que vous lui imposerez (8 jours par exemple).

En cas d'échec (absence de réponse ou réponse négative), vous pouvez alors exercer votre droit à l'annulation de la vente dans les conditions ci-dessus énoncées.

- **Commande incomplète**

Si votre commande n'est pas complète, vous pouvez toujours contacter le cyber-vendeur pour exiger les articles manquants.

Si le professionnel est dans l'impossibilité de vous les fournir, vous pouvez obtenir une réduction du prix payé, voire un remboursement total de votre commande si ces produits sont indispensables.

- **Commande défectueuse**

Si vous constatez des anomalies concernant l'état de la commande, n'hésitez pas à apposer des remarques dans la partie « réserves » du bon de livraison.

Dans cette hypothèse, adressez un courrier de réclamation en recommandé avec accusé de réception au transporteur dans les 3 jours de la réception de la commande. Prévenez également le cyber-vendeur de votre problème. Ainsi, si votre colis est endommagé ou cassé, il sera plus facile d'obtenir une réparation.

A la livraison, vous devez, dans la mesure du possible, vérifier le contenu et l'état de votre colis

En cas de problème, il vous suffira de refuser la livraison de la commande (retour à l'expéditeur). Si vous découvrez une anomalie après la livraison, retournez rapidement l'article commandé au professionnel, de préférence dans son emballage d'origine.

En cas de litige avec un cyber-marchand

Le professionnel est situé en France

Il est conseillé dans un premier temps de rechercher une solution amiable. Contactez le service compétent (service consommateur, service clientèle ou service réclamation...) dont les coordonnées figurent en général sur le site du professionnel ou dans les conditions générales de vente. À défaut de solution par téléphone, adressez un courrier recommandé au professionnel en expliquant les faits et en joignant toutes les pièces justificatives.

Si cette démarche n'aboutit pas, et si le site marchand est adhérent à la Fédération du e-commerce et de la vente à distance (FEVAD), vous pouvez solliciter le service médiation de la FEVAD qui intervient auprès de la société membre pour tenter de trouver une solution au litige.

Pour la contacter, il suffit de lui écrire en exposant les faits :



- **Soit par e-mail à**
mediateurduecommerce@fevad.com
- **Soit par courrier postal à**
 Médiateur du e-commerce -
 60 Rue la Boétie – 75008 PARIS
- **Soit via le formulaire en ligne**
www.mediateurfevad.fr

Le professionnel est situé dans l'Union européenne, en Norvège ou en Islande

En cas de litige avec un professionnel situé dans l'Union européenne, vous pouvez solliciter l'aide du Centre européen des consommateurs (CEC). Cette démarche est entièrement gratuite et vous permet de surmonter la barrière de la langue.

Le CEC est composé d'antennes nationales (centres d'accueil et d'information) présentes sur l'ensemble du territoire européen. En votre qualité de consommateur résidant en France, vous devez saisir le point de contact national du CEC France pour que celui-ci entame des démarches en vue du règlement amiable de votre dossier, soit auprès du médiateur compétent dans l'Etat membre, soit directement auprès du professionnel.

Ses coordonnées sont les suivantes :



CEC France

Rehfusplatz 11

77694 KEHL

Allemagne

Tel : 0049 7851 991 48 0

Email : info@euroinfo-kehl.eu

Le saviez-vous ?

Tout au long de vos démarches, sachez que vous pouvez obtenir des renseignements ou bien vous faire assister par notre association de défense des consommateurs.

Mémo

10 éléments à retenir quand vous réalisez un achat sur Internet

- 1 Les règles et les garanties applicables lors de l'achat d'un produit ne sont pas les mêmes si vous achetez auprès d'un particulier ou d'un professionnel
- 2 Lors de l'achat sur un site marchand, vérifiez la fiabilité du site (les coordonnées du commerçant se trouvent facilement, les conditions générales de vente sont accessibles...)
- 3 En général, si le produit commandé ne vous convient pas, vous avez **un délai de 14 jours à compter de sa réception** pour changer d'avis. Pour les prestations de service, le délai de 14 jours court à compter de **la validation de la commande**
- 4 Avant d'engager des achats sur Internet, vérifiez que vous êtes bien sur un site protégé : préfixe https et icône du cadenas fermé.
- 5 Faites un suivi rapproché du débit de votre carte bancaire si vous utilisez ce moyen de paiement
- 6 À la livraison, vous devez, dans la mesure du possible, vérifier le contenu et l'état de votre colis
- 7 Lors de l'achat d'un bien, vous disposez de plusieurs garanties. Certaines sont prévues par la loi et d'autres par le vendeur
- 8 En cas de litige avec le cybermarchand, faites d'abord une réclamation par courrier recommandé au service clientèle/consommateur
- 9 En cas d'échec, vous pouvez saisir le médiateur du e-commerce
- 10 Si le professionnel est situé hors de France, mais dans l'Union européenne, en Norvège ou en Islande, vous pouvez saisir le CEC France

À l'heure de l'ère numérique, où plus de 58% de la population française, soit 38,2 millions de personnes, sont des internautes, il est incontestable que nos pratiques de consommation quotidiennes ont fondamentalement évoluées.

Si Internet donne l'apparence d'une fenêtre ouverte sur le monde, d'une grande liberté de parole et d'action où en quelques clics chacun peut discuter avec ses amis, suivre l'information en continu, comparer les prix des produits et services, il ne faut pas oublier que cette fenêtre est aussi un puissant outil d'observation constituant une véritable passerelle d'accès à notre vie privée avec tout ce que cela implique de pratiques qui parfois peuvent être abusives.

Ainsi, ce guide réalisé par l'Association Léo Lagrange pour la défense des consommateurs a pour objectif d'éveiller votre vigilance concernant les pièges qui vous attendent quand vous êtes connectés à Internet, et vous transmettre quelques bons réflexes et conseils qui vous mettront à l'abri du pire tout en gardant bien à l'esprit que la sécurité absolue n'existera jamais.

Bonne lecture à tous !

L'Association Léo Lagrange pour la défense des consommateurs (ALLDC), association nationale de consommateurs agréée, apporte aux citoyens, information, conseil et aide juridique. Elle met aussi en œuvre différents leviers au niveau collectif tels que la négociation à l'échelon national ou européen pour l'élaboration de nouvelles normes et règles du jeu, ou la participation aux campagnes nationales d'information et de sensibilisation (surendettement, commerce équitable, agriculture durable...).

Association Léo Lagrange pour la défense des consommateurs

150 rue des Poissonniers

75883 Paris cedex 18

Tél : 01 53 09 00 00

consom@leolagrange.org

www.leolagrange-conso.org