Les bases de la sécurité numérique

Être à l'aise avec un ordinateur n'est pas toujours évident et c'est l'expérience qui vous apportera confiance en vous et maîtrise. Mais au-delà de l'expérience, il y a des éléments à connaître pour **évoluer sereinement dans un environnement numérique**.

Internet nous permet d'être connecté partout dans le monde et auprès de n'importe qui. C'est extraordinaire ! Mais cette **hyper connexion nous expose à un certain nombre de risques** : virus, escroquerie, vol de données personnelles, usurpation d'identité...

Je vous propose dans ce cours d'apprendre à **protéger vos données personnelles** en identifiant les **actions malveillantes** et en appliquant les **bonnes pratiques de sécurité**, pour vous éviter quelques déboires, et que votre navigation sur Internet soit un plaisir !

Détectez les tentatives d’hameçonnage

Bienvenue dans notre premier chapitre ! 

Pour commencer ce cours, nous allons définir ce qu’est le « phishing ».

Découvrez le principe de l'hameçonnage (ou *phishing*, en anglais)

Le terme "**phishing**" correspond à la contraction des mots anglais "fishing" qui signifie "pêche" et "phreaking" qui veut dire "piratage de lignes téléphoniques".

En français, on parle d’**hameçonnage** ; il s’agit d’une technique de piratage destinée à récupérer des informations personnelles, et qui consiste, pour le fraudeur, à se faire passer pour une administration ou une entreprise dont vous êtes familier (banque, service des impôts, CPAM, etc.).

> Cet e-mail contient **un lien sur lequel on vous invite à cliquer**, le plus souvent pour des raisons de sécurité, afin de vous connecter à un site ou à un formulaire **où l’on vous demandera de remplir différents champs**.

> Ce lien vous conduit en réalité vers un **site pirate**. Les champs que le pirate souhaite vous voir remplir sont pour lui le moyen de vous **soutirer des informations**.

Les objectifs du phishing

L’objectif de l’expéditeur de cet e-mail est de vous pousser à agir vite, sans prendre le temps de réfléchir.

Par ce biais, il pourra par exemple **tenter de récupérer vos identifiants et mots de passe** sur un compte commercial (pour passer des commandes en votre nom), ou bien vos codes d’accès à votre banque en ligne (afin de dérober de l’argent), ou toute autre information personnelle pouvant lui être utile.

> Je vous donnerai davantage d’exemples concrets sur les tentatives de phishing dans la suite de ce chapitre. Restez avez moi !

Repérez les indicateurs du danger

Pour ne pas devenir victime d’une tentative de phishing, vous découvrirez ci-dessous les différents éléments qui doivent **éveiller votre méfiance**.

L'objet de l'email

Le pirate, déguisé en tiers de confiance, vous envoie par exemple un mail avec un objet :

- alarmiste, à caractère **urgent et problématique** (compte bloqué, facture impayée, etc.) :

« *urgent* », « *compte suspendu* », « *problème sur votre compte* » ou encore « *accès restreint* » ;

- insistant sur un **gain potentiel** (remboursement d'une facture, gain d'un concours) :

« *Retirez votre gain* », « *Bon d'achat à l'intérieur* » ;

- **exagérément optimiste** :

« *Confidentiel – plus que 24 h pour retirer votre voyage* ».

Les fautes d'orthographe

Des fautes d'orthographe et/ou des erreurs de grammaire ou de syntaxe prouvent à coup sûr qu'il s'agit d'un mail frauduleux. Malheureusement, l'inverse n'est pas vrai : l'absence de faute d'orthographe, de grammaire ou de syntaxe n'est pas suffisante pour garantir qu'un mail est sans danger.

La demande d'informations personnelles

L'expéditeur demande que vous lui transmettiez des informations personnelles et/ou confidentielles (identifiant, mot de passe) ou encore des documents privés, comme une pièce d'identité ou un RIB.

Ne communiquez jamais vos numéros de carte bancaire, identifiant ou mot de passe, par exemple, en cliquant sur un lien contenu dans un courrier électronique.

Dès lors qu'il s'agit d'entrer ce type d'informations :

- ouvrez votre navigateur Internet ;
- rendez-vous sur la page d'accueil du site concerné ;
- connectez-vous à votre compte en toute sécurité.

Les liens

L'adresse de l'expéditeur ou le site vers lequel vous êtes redirigé sont approximatifs :

Vous lisez par exemple, l'URL : opencassroom.com; alors que vous savez que la véritable adresse est https://openclassrooms.com.

Un conseil : avant de cliquer sur un lien, passez simplement votre souris dessus, vous verrez s'afficher dans le coin à gauche de votre écran, l'URL du site Internet qui se cache derrière le lien :

Exemple d'un écran

Le lien comporte une longue série de chiffres et de lettre, comme cela : « http://www.CoursXMQXfuXKtWR8gKa5oGACg.fr »

Le message comporte des **liens qui ne fonctionnent pas**.

Découvrez des exemples de courrier d'hameçonnage

Exemple 1

Supposons que vous receviez un courrier électronique ayant pour objet « *Alerte intrusion – Urgent* » et vous avertissant que, pour des raisons de sécurité, votre banque invite l'ensemble de ses clients à modifier leur code d'accès dans un délai de 24 h sous peine de ne plus pouvoir se connecter à leur espace personnel.

Inquiet à l'idée de perdre l'accès à votre banque en ligne, vous cliquez aussitôt sur le lien indiqué !

Un formulaire s'affiche, il comporte le logo de votre banque, et il vous demande de taper vos informations de connexion pour ensuite définir un nouveau mot de passe. Vous remplissez les champs comme demandé, puis vous cliquez sur « OK ».

Aïe ! Vous venez de confier aux pirates le code d'accès à votre banque !

Dans un tel cas, il est important de savoir qu'**une vraie banque ne procède jamais ainsi**. Il s'agit donc bien d'une **tentative de phishing** : le mail a été envoyé par un pirate, parti à la « pêche aux victimes » !

Sachez qu'une administration ou toute entreprise légale ne vous demandera jamais de renseigner vos informations personnelles sur une page Internet à laquelle vous avez accès **sans vous y être inscrit au préalable en utilisant un nom d'utilisateur et un mot de passe**.

Exemple 2

Une tentative de phishing peut aussi se présenter sous la forme d'un e-mail vous avertissant que vous êtes **redevable d'une amende** qui doit être **réglée sans délai**, sous peine de poursuites.

> Il contient, par exemple, un lien permettant de régler votre amende en ligne et provenant d'un soi-disant site du gouvernement.

En cas de doute, ne cliquez jamais sur le lien envoyé ; faites une recherche pour vérifier l'adresse du site : en tapant « paiement amende en ligne gouvernement » sur un moteur de recherche. Vous trouverez par exemple l'adresse www.amendes.gouv.fr/tai

Vous ne trouvez pas sur votre moteur de recherche, le lien envoyé par email ? C'est probablement que celui-ci vous aurait conduit à un site pirate, ressemblant fortement au site officiel, mais conçu dans le seul but de récupérer vos données ; comme votre numéro de carte bancaire par exemple.

> Pour information un site du gouvernement se terminera par ".gouv.fr"

Exemple 3

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GENERALE DES FINANCES PUBLIQUES 01/09/2010

Notification d'impôt - Remboursement

Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement d'impôt de € 178,80.

S'il vous plaît soumettre la demande de remboursement d'impôt et nous permettre de 10 jours ouvrables pour le traitement.

Pour accéder au formulaire pour votre remboursement d'impôt, cliquez ici

Un remboursement peut être retardé pour diverses raisons. Par exemple la soumission des dossiers non valides ou inscrivez après la date limite.

Le Conciliateur fiscal adjoint

E-mail d'hameçonnage se faisant passer pour le service des impôts, contient des erreurs de syntaxe

Exemple 4

Le graphisme de ce mail a un aspect vieillot et si l'on survole les boutons « Particuliers » et « Mon compte »

avec la souris, on s'aperçoit qu'ils pointent vers l'adresse http://dasnova.com,un site qui n'a rien à voir avec la CAF !

Exemple 5

Votre chargé de clientèle

Bonjour,

Lors de votre dernier achat , vous avez été averti par un message vous informant de l'obligation d'adhérer à la nouvelle réglementation concernant la
fiabilité pour les achats par C.B. sur internet et de la mise en place d'un arrêt pour vos futurs achats.

Or, nous n'avons pas, ce jour, d'adhésion de votre part et nous sommes au regret de vous informer que vous pouvez plus utiliser votre carte sur internet.
Nous vous invitons à en prendre connaissance : Adhésion : Faites votre demande d'adhésion en ligne en cliquant ici

Ce mail provenant de "La Banque Postale" mentionne en objet : "*Assurer la sécurité des informations qui vous concernent*". En vérifiant l'adresse e-mail, de l'expéditeur, on peut lire : *static.feet986JGO5E876HJF76@telegenic.co.uk.*

Ce type d'adresse, incluant des suites de chiffres et de lettres, doit systématiquement éveiller votre méfiance.

Exemple 6

BNP PARIBAS

Cher client de **BNP Paribas**,

Le département technique de BNP Paribas procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.secure.bnpparibas.net/banque/portail/confprocedure.asp

Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

La tournure de phrase utilisée dans ce mail est très inhabituelle…
Les procédures utilisées par les banques sont extrêmement sécurisées ; aucune banque ne vous demandera de confirmer des informations par le biais d'un mail.

Réagissez face à une tentative d'hameçonnage

Si vous reconnaissez une tentative d'hameçonnage :

- ne cliquez jamais sur les liens présents dans le mail ;
- ne répondez pas au message ;
- n'ouvrez surtout pas les fichiers envoyés en pièces jointes ;
- signalez le message comme « courrier indésirable » (si cette fonctionnalité est accessible dans votre messagerie) ;
- prévenez l'administration ou l'entreprise concernée (banque, agence de location de vacances, Caisse d'allocations familiales, etc.) et transférez le mail à leur service client ;
- pour finir, supprimez le courrier.

Il existe un moyen très simple pour vous prémunir contre les tentatives de phishing : l'**installation d'un antivirus** couplée à celle d'un **pare-feu** constitue en effet une protection efficace dans la majorité des cas.

Nous verrons cela dans la dernière partie de ce cours (« Protégez votre ordinateur »).

Que faire si je suis victime de phishing ?

Malgré toutes les précautions prises, vous avez cliqué sur un lien contenu dans un courrier ? Ce lien vous a amené jusqu'à une page de connexion sur laquelle vous avez saisi vos identifiant et mot de passe, pour vous apercevoir après coup que vous avez été victime d'hameçonnage : heureusement, il est encore temps de contrecarrer les projets des pirates ! 

Vous devez pour cela **contacter le plus rapidement possible l'administration ou l'entreprise** concernée afin de bloquer l'accès à votre compte :

- modifiez immédiatement les identifiant et mot de passe du service concerné ;
- si le phishing est lié à votre compte bancaire, contactez votre banque le plus rapidement possible afin de les en avertir ; elle pourra alors prendre les mesures nécessaires pour protéger vos comptes.

Pour lutter contre ce phénomène, le gouvernement a mis à la disposition des internautes un site leur permettant de signaler toute tentative d'hameçonnage, fraude ou escroquerie.

N'hésitez pas à effectuer un signalement sur le **portail officiel de contenus illicites sur Internet** : **www.internet-signalement.gouv.fr**.

D'autre part, les administrations ou les grandes entreprises publient régulièrement des alertes de sécurité : pensez donc également à consulter les sites concernés.

Supposons par exemple que vous receviez un mail « *Urgent* » de Microsoft vous invitant à télécharger un fichier pour mettre à jour votre système, afin d'éviter une interruption imminente de leurs services : ne cliquez en aucun cas sur le lien que l'on vous envoie !

Connectez-vous plutôt sur la page d'accueil de Microsoft : il est en effet fort possible qu'une alerte ait été diffusée afin d'avertir les utilisateurs de cette tentative de phishing.

Les sites bancaires, tout comme ceux des impôts, de la Caisse d'allocations familiales et bien d'autres, sont également susceptibles de diffuser de telles alertes.

En résumé

- Le **phishing**, aussi appelé ***hameçonnage***, est une technique de piratage destinée à récupérer des données personnelles qui seront ensuite exploitées par les pirates.
- Une tentative de phishing prend la forme d'un mail, dont l'objet présente un caractère urgent, et qui semble le plus souvent provenir d'une administration ou d'une entreprise dont vous êtes familier.
- Différents éléments peuvent vous alerter, comme la présence de fautes de français, l'objet du mail, l'adresse de l'expéditeur qui ne correspond pas à celle de l'expéditeur officiel, des liens qui ne fonctionnent pas, etc.
- Pour ne pas devenir victime, ne communiquez jamais d'informations confidentielles en cliquant sur un lien contenu dans un courriel.
- Si vous reconnaissez une tentative d'hameçonnage : ne cliquez pas sur les liens indiqués, ne répondez pas au message, mais prévenez l'organisme concerné, signalez l'e-mail comme indésirable et supprimez-le.

Reconnaissez les e-mails indésirables ou dangereux

Vous avez peut-être déjà été confronté à ces e-mails indésirables, « spams » ou « bots », qui trop souvent encombrent nos boîtes de réception. Et qu'en est-il des pièces jointes indésirables ?

Je vous propose dans ce chapitre d'apprendre à les identifier.

Identifiez les types de mails frauduleux

Le spam

> Qu'est-ce qu'un spam ? Pourquoi les reçoit-on dans nos courriers électroniques ? Comment faire pour éviter de recevoir ces courriers indésirables ?

> Un spam (ou *courrier indésirable*) est un courrier électronique qui n'a été ni demandé, ni souhaité par le destinataire.

Ces courriers sont **envoyés à un très grand nombre de personnes** : ils représentent plus de 3/4 des e-mails envoyés à travers le monde. La majorité d'entre eux est composée de courriels indésirables tels les e-mails publicitaires, ou encore les « chaînes de lettres ». Bien qu'envahissant, ce type de spam demeure **inoffensif**.

> Mais un spam peut aussi se présenter sous la forme d'une **tentative d'escroquerie ou d'hameçonnage**, bien plus dangereuses pour le destinataire.

Le bot

Le « bot », moins connu du grand public, est pourtant lui aussi **largement répandu**.

> Le terme « bot » est la **contraction** du mot anglais « robot ».

> À l'origine, les bots sont des **programmes informatiques** développés pour effectuer des **tâches répétitives**. Un « bot » est aujourd'hui utilisé pour désigner un programme conçu pour **répondre automatiquement aux courriers** envoyés par les clients ou consommateurs.

Lorsque vous réalisez un **achat sur internet**, il arrive fréquemment que dans les minutes qui suivent votre commande, vous receviez un mail du type :

> *« Bonjour,*

Nous vous remercions de votre commande. Nous vous tiendrons informés par e-mail lorsque les articles de votre commande auront été expédiés. Votre date de livraison estimée est indiquée ci-dessous. Vous pouvez suivre l'état de votre commande ou modifier celle-ci dans Vos commandes sur votre espace client. »

Ce type de mail n'est pas envoyé par un employé du site sur lequel vous avez passé commande ? Mais par un programme informatique conçu pour cela : un **bot**.

Certains bots ont donc une **réelle utilité**, tels les bots qui envoient des **confirmations de commandes** ou encore les bots d'indexation des moteurs de recherche (qui sont chargés de parcourir le web et d'analyser les informations trouvées, permettant ainsi aux moteurs de recherche de vous proposer des résultats).

Mais il existe de « mauvais bots », comme les « **spambots** », utilisés par les spammeurs (c'est ainsi que l'on nomme les expéditeurs de spams) pour parcourir le web afin de **récolter le plus grand nombre possible d'adresses mail** (dénichées sur des sites web, des forums de discussion ou des réseaux sociaux). Une fois les adresses récupérées, les **spambots** sont programmés pour envoyer des spams à ces adresses e-mail.

Les différentes formes de spam

Afin de mieux les discerner, vous trouverez ci-dessous les grandes catégories de spam, chacune assortie d'un exemple. Un spam peut ainsi prendre la forme de :

Mails publicitaires (forme la plus courante)

Découverte de Pilules Minceur !!!
Et si vous pouviez vraiment perdre 2, 5 ou même 10 kg, de manière sûre et rapide, en moins de 30 jours ?
MAINTENANT, C'EST POSSIBLE !
Pour en savoir plus, cliquez sur le lien suivant.

Fausses informations/tentatives d'escroquerie

On les appelle également *scams*.

L'expéditeur peut par exemple proposer de vous vendre une méthode « miracle » pour vous enrichir rapidement :

« *Est-ce vous connaissez cette histoire incroyable ?*

Une Youtubeuse vend l'eau de son bain à ses fans pour 10.000 $!
Cela montre bien que nous vivons une époque incroyable où les opportunités de gagner de l'argent en faisant ce qu'on aime abondent.

Par contre, vous n'avez pas à vendre l'eau de votre bain pour vivre la vie riche et libre que vous méritez. Il vous suffit de suivre cette méthode que je vous offre gratuitement (ebook et vidéos) :
Découvrez cette méthode gratuite pour devenir libre et démultiplier *votre richesse ! (lien) »*

Chaînes de lettres

« Cette prière t'est envoyée pour te porter chance. L'original vient des Pays-Bas. Elle a fait neuf fois le tour du monde. La chance t'est envoyée. Il t'arrivera un événement heureux dans les neuf jours qui suivront la réception de ce message. Ceci n'est pas une plaisanterie. Envoie 20 copies de ce message à des gens qui ont besoin de chance. ... Zorin Barrachilli a reçu ce courrier. Il ne l'a pas cru, et l'a supprimé. Neuf jours plus tard, il est mort. Cette chaîne ne doit être interrompue sous aucun prétexte. ».

Hameçonnage

« Il est venu à notre attention que vos PayPal informations dossiers ne sont plus à jour. Le fait de ne pas mettre à jour vos enregistrements en compte de résiliation. S'il vous plaît mettre à jour vos dossiers dans les 24 heures. Une fois que vous avez mis à jour votre compte, votre PayPal session ne sera pas interrompu et continuer comme d'habitude. Le défaut de mise à jour en conséquence annulation de service, Conditions de service (TOS) violations ou à venir problèmes de facturation.
Vous devez cliquer sur le lien ci-dessous et entrez vos informations de connexion sur la page suivante pour confirmer vos informations de facturation.

J'accepte. Mettre a Jour mon Identifiant

».

Vous recherchez un logement à louer pour vos vacances ? Lors de vos recherches, il est fort probable qu'une fenêtre apparaisse, vous proposant de renseigner votre adresse mail afin de recevoir des offres similaires. Vous participez à un jeu-concours sur Internet ? Il vous sera demandé d'indiquer votre adresse mail !

De même lorsque vous créez votre compte client sur un site de vente en ligne, un réseau social ou un forum de discussion, vous devez là aussi fournir votre adresse mail.

Votre adresse est ainsi enregistrée dans un nombre sans cesse croissant de bases de données (ou listes) ; ces listes d'adresses peuvent ensuite être revendues par leurs propriétaires à des fins publicitaires.

En outre, et comme nous l'expliquions un peu plus haut, votre adresse mail peut aussi être récupérée à votre insu, puis ciblée par un spambot.

Les règles de base pour les éviter

À cause des énormes quantités de spams en circulation et de la fréquence à laquelle ils sont envoyés, il est malheureusement impossible d'être protégé à 100 % (contre la réception de spams).

Les quelques conseils ci-dessous vous permettront cependant de restreindre le nombre de spams arrivant dans votre boîte de réception.

Évitez de communiquer votre adresse mail

La meilleure protection serait en effet de ne communiquer votre adresse qu'avec la plus grande parcimonie.

Toutefois, si vous devez absolument la renseigner, pour créer votre compte sur un site commercial ou un forum de discussion par exemple, prenez le temps de consulter la rubrique « ***Vie privée et cookies*** » : un site fiable doit normalement vous donner la possibilité de refuser la communication de vos données (dont votre adresse mail) à d'autres entreprises.

> Ainsi, le site *Le Bon Coin* indique, par exemple : « nous sommes susceptibles, avec votre consentement : de partager vos données à nos partenaires publicitaires, responsables de traitement, aux fins d'améliorer les performances des campagnes de nos partenaires sur notre site. Vous pouvez à tout moment ***paramétrer et refuser ce partage de données****, en cliquant ici : [Lien]* ».

« Déguisez » votre adresse

Vous souhaitez, par exemple, donner votre adresse sur un blog. Pour éviter que votre adresse ne soit collectée par des robots d'indexation, vous pouvez la « déguiser » en remplaçant le symbole @ par les lettres « AT » ou encore le « . » par le mot « Point »:

> albertdupond**@**yahoo**.**com peut ainsi devenir albertdupond**AT**yahoo**.**com ou encore albertdupond@yahoo**POINT**

> De tels changements sont susceptibles de leurrer un programme informatique (spambot) tout en restant compréhensibles par un être humain.

Créez plusieurs adresses mails

Une astuce largement répandue chez les internautes consiste à **créer et utiliser 2 adresses mail** :

- **une adresse principale**, que vous ne communiquerez qu'à vos proches, et à des organismes fiables comme votre banque, la Caf, la Sécurité sociale ou encore le site des impôts ;

- et une seconde adresse, dédiée à tous les autres sites : inscription à des forums de discussion, création de vos comptes clients sur des sites de vente en ligne, inscription sur les réseaux sociaux, etc.

Il est tout à fait possible de décliner cette méthode en créant plus de 2 adresses.

Les filtres anti-spam

Un filtre anti-spam est un logiciel capable de reconnaître les courriers indésirables : au moment où les mails arrivent dans votre boîte aux lettres, le filtre va placer les messages qui lui semblent inoffensifs dans votre boîte de réception, et ranger dans un dossier séparé nommé « Spams » ou « Indésirables » tous les mails lui paraissant appartenir à cette catégorie.

Les webmails ou services de messagerie

Vous avez par exemple comme webmail : Hotmail, Gmail, Yahoo, ProtonMail.

Ces webmails ainsi que les logiciels dédiés au courrier électronique (comme Outlook), sont tous équipés d'un filtre antispam. Grâce à cela, la majorité des spams que vous recevez n'arrivent pas jusqu'à votre boîte aux lettres.

Mais un petit nombre de courriels non désirés apparaîtra tout de même dans votre boîte de réception. Vous avez alors la possibilité de paramétrer le filtre antispam existant, pour lui signaler les spams qu'il n'a pas détectés en amont. Dans votre liste de messages, recherchez dans les paramètres (par un clic droit sur le mail concerné ou dans un menu Paramètres) des actions comme : « *Ajouter aux indésirables* » ou « *Ajouter à la liste des expéditeurs bloqués* ».

À l'inverse, il arrive parfois que des mails que vous attendez se retrouvent par erreur dans le dossier spam. Il est préférable dans ces cas-là de signaler au filtre antispam que ce **courrier est légitime**. Il suffit en général pour cela de cliquer dans les paramètres de l'e-mail concerné sur : « *Ajouter aux expéditeurs approuvés* », ou encore « *signaler comme courrier légitime* ».

Signaler un spam

Selon l'article L.34-5 du Code des postes et des communications électroniques, il est interdit d'envoyer des messages publicitaires ou commerciaux sans l'accord préalable du destinataire.
Les signalements fournissent aux autorités (représentées dans ce cas par la CNIL, ou *Commission nationale de l'informatique et des libertés*) la preuve nécessaire pour effectuer des contrôles (assortis d'éventuelles sanctions) envers les sociétés émettrices d'e-mails publicitaires, et des actions en justice contre les cybercriminels.

Toute personne ayant reçu un spam peut le signaler sur le site : **www.signal-spam.fr**

Identifiez les pièces jointes malveillantes

Que ce soit pour partager quasi-instantanément des photos de famille, des documents de travail, ou pour des démarches administratives, l'échange de fichiers par mail, facile et rapide, est aujourd'hui largement répandu.

> Qu'est-ce qu'une pièce jointe piégée ou vérolée ? Comment la discerner d'une pièce jointe inoffensive ?

Une pièce jointe est un fichier joint à un courrier électronique. Vous reconnaîtrez facilement les mails qui en contiennent au petit **trombone** apparent sur la ligne du message dans votre boîte de réception.

Exemple d'un e-mail avec une pièce jointe

Il existe ainsi de nombreuses sortes de pièces jointes : photos, documents modifiables ou non, etc. Heureusement, **la plupart sont inoffensives**, mais il arrive que certaines de ces pièces soient piégées ou vérolées : cela signifie que le fichier envoyé **contient un virus**, c'est-à-dire un programme informatique dont l'objectif est d'**endommager votre ordinateur** (ralentir, ou même empêcher son fonctionnement), ou de vous d**érober des données personnelles** (identifiants, mots de passe, codes d'accès…). Les pirates cherchent ainsi à faire passer des programmes contenant des virus pour des fichiers tout à fait communs et inoffensifs (document PDF ou Word, image JPG ou autre).

> Comment se protéger des virus ? 🤔
>
> Vous en saurez plus sur les moyens de s'en protéger dans la suite de ce cours (chapitre 3.2, « Protégez votre ordinateur »).

Les pièces jointes envoyées par mail représentent le **principal accès emprunté par les virus** pour s'attaquer à nos ordinateurs.

Ainsi, si vous recevez un mail semblant provenir d'un site de vente en ligne ou de tout autre service (d'un expéditeur que vous ne connaissez pas personnellement), et **vous invitant à installer un programme** pour, par exemple, activer le suivi d'une commande, il s'agit probablement d'un **logiciel malveillant** : **les sites fiables ne vous demanderont jamais d'installer un logiciel par le biais d'un e-mail**.

De même, un courrier vous annonçant que vous êtes l'heureux gagnant d'une loterie ou d'un concours, et vous enjoignant d'ouvrir une pièce jointe pour valider votre gain, représente certainement une menace pour la sécurité de vos données et de votre ordinateur.

Il est malheureusement facile de s'y laisser prendre, car **les e-mails sont de plus en plus crédibles**. Il suffit de quelques minutes d'inattention :

L'une de ces arnaques circulant sur Internet consistait à envoyer un mail annonçant à son destinataire qu'il était « l'heureux » gagnant d'un billet d'avion. Le courrier empruntait le logo et le style d'une célèbre compagnie d'aviation et semblait tout à fait sérieux.

Il contenait un fichier nommé *Validation_Billet.htm* en pièce jointe.

Cette escroquerie a particulièrement bien fonctionné avec les personnes âgées ou peu habituées à l'outil informatique : lorsque le destinataire, **par curiosité**, cliquait sur la PJ, une sonnerie extrêmement forte, comparable à celle d'une alarme, retentissait (elle provenait de l'ordinateur) et un message occupant la totalité de l'écran s'affichait : « *Alerte sécurité ! Votre système a été infecté par un virus. Appelez immédiatement ce n° de téléphone* ».

La sonnerie très puissante, qui durait plusieurs minutes, augmentait encore la panique de l'utilisateur qui sans réfléchir appelait le numéro indiqué. Son interlocuteur lui enjoignait alors de faire une manipulation officiellement destinée à « débloquer l'ordinateur » mais qui en réalité, lui permettait de **prendre à distance le contrôle de la machine**. Il pouvait ensuite dérober toutes les données qu'elle contenait ou bien la contaminer avec un virus.

Qui a envoyé l'e-mail ?

Pour déterminer si une pièce jointe est dangereuse ou non, la première chose à faire est de vérifier l'identité de l'expéditeur : la meilleure règle de conduite à adopter serait de **ne jamais ouvrir une pièce jointe dont l'expéditeur est inconnu**.

D'une manière générale, **tout courrier vous incitant à ouvrir une pièce jointe** doit donc vous sembler **suspect**, à moins que vous ne connaissiez personnellement son expéditeur.

Et même dans ce cas, vous devez néanmoins prendre le temps d'observer le contenu du message avant d'ouvrir le fichier joint. **Il est en effet possible que l'expéditeur ait lui-même été victime de piratage** ; c'est alors sans le vouloir, et sans en avoir conscience, qu'il peut vous envoyer un e-mail infecté.

Lisez donc attentivement le courrier afin de vérifier la cohérence entre son expéditeur et son contenu, et si quelque chose vous parait inhabituel, n'hésitez pas à contacter directement la personne qui semble l'avoir envoyé.

S'il est logique qu'un membre de votre famille ou un ami vous envoie des photos ou encore un document que vous lui aviez demandé, cela le serait moins qu'il ou elle vous transmette un programme sans vous en avoir parlé auparavant : la suite de ce cours vous apprendra justement à distinguer les différents types de fichiers que l'on peut trouver en pièces jointes, grâce à leur extension.

Observez l'extension de la pièce jointe

Tout fichier possède à la fois un nom et une extension : l'extension d'un fichier se compose de 3 ou 4 lettres, séparées de son nom par un point.

Par exemple :

- *mondocument**.DOCX*** indique qu'il s'agit d'un fichier texte que l'on peut ouvrir, lire et modifier, à l'aide du logiciel Microsoft Word ;
- *mondocument**.PDF*** désigne également un document, mais l'extension PDF indique que vous pourrez uniquement le consulter et non le modifier.

Les fichiers correspondants à des programmes – ceux susceptibles de contenir un virus – s'accompagnent de l'extension **.EXE** : ces trois lettres doivent donc éveiller votre méfiance.

Outre les .exe, d'autres extensions peuvent être indicatrices de danger : ainsi, il vaut mieux ne pas ouvrir de fichiers ayant pour extension **.msi**, .**bat** ou encore **.cmd**.

À l'inverse, certaines extensions de fichiers nous garantissent heureusement que ces derniers sont sans danger ; il s'agit par exemple des : **.gif, .jpg, .jpeg, .png, .mp3, .mp4** et **.wav** qui désignent des images vidéo ou musiques.

Cependant, **les pirates tentent parfois de les utiliser pour masquer l'envoi d'un virus** : une pièce jointe nommée *Image.Png.Exe* contient plus probablement un programme malveillant qu'une véritable image. Sachez que **les doubles extensions sont anormales** ; n'ouvrez pas les fichiers qui en seraient munis, mais au contraire **supprimez-les**.

De même, si les .txt, .doc**x**, .ppt**x**, .xls**x** et .pdf accompagnent des fichiers inoffensifs, les .doc**m**, .xls**m** et .ppt**m** peuvent être dangereux.
La dernière lettre de l'extension (le m signifiant « macro ») indique en effet que ces fichiers contiennent un programme.

D’autre part, lorsque les pièces jointes sont trop nombreuses ou trop volumineuses, elles sont envoyées dans des **fichiers compressés**, ce qui permet de réduire leur taille. Ce type de fichier affiche une extension **.zip** ou **.rar** : s’il vous arrivait d’en recevoir, sachez qu’ils peuvent être tout à fait inoffensifs. Si vous connaissez l’expéditeur et si vous êtes prévenus de cet envoi, vous pouvez donc les ouvrir sans crainte, sous réserve d'avoir bien vérifié l’identité de la personne qui vous les envoie, puisque là encore des pirates peuvent utiliser des extensions pour dissimuler des codes malveillants.

En cas de doute, vous pouvez bien entendu effacer le message et toutes ses pièces jointes, mais si vous craignez de supprimer ainsi des documents importants, vous avez également la **possibilité d’analyser ces fichiers** : soit grâce à votre **antivirus**, soit en utilisant « VirusTotal », un service disponible gratuitement sur Internet.

Si, par malchance, vous étiez tout de même victime un jour d’une pièce jointe contenant un virus, cela ne veut pas dire pour autant que votre ordinateur sera forcément infecté ou vos données personnelles dérobées ; **un bon antivirus doublé d’un pare-feu sont en effet des protections efficaces** qui se chargeront de **bloquer le programme malveillant** dès l’ouverture du fichier.

> Pour savoir comment les choisir et les installer, et assurer ainsi la sécurité de votre ordinateur et de vos données, rejoignez-moi dans la troisième partie de ce cours !

En résumé

- Un spam est un courrier que son destinataire n’a pas souhaité recevoir (courrier « indésirable »).
- Un bot est un programme chargé de répondre automatiquement aux messages des clients et consommateurs.
- La grande majorité des spams sont inoffensifs ; cependant, parmi les différentes catégories de spams, on retrouve les scams (*tentatives d’escroquerie*) et les mails d’hameçonnage (ou *phishing*).
- Pour éviter les spams : ne communiquez votre adresse mail qu’avec parcimonie. Et si vous devez absolument la communiquer, déguisez-la ou bien créez et utilisez plusieurs adresses mail, chacune d’entre elles étant dédiée à un rôle bien précis.
- Pour savoir si la pièce jointe que vous avez reçue est dangereuse ou non, soyez attentif à l’identité de l’expéditeur et à l’extension du fichier.
- N’ouvrez jamais les pièces jointes qui vous paraissent dangereuses ou même simplement douteuses ; supprimez le mail et les fichiers joints.

Naviguez sur Internet en toute sécurité

Nous sommes nombreux aujourd'hui à effectuer des achats sur Internet. On y trouve en effet un vaste choix de produits et services à des prix souvent plus intéressants que dans les magasins.

Avant de réaliser un achat en ligne, nous comparons généralement les prix afin de dénicher la « bonne affaire », le rapport qualité-prix le plus intéressant.

> Ce procédé, en nous poussant à visiter toujours plus de sites à la recherche de la meilleure opportunité, est toutefois susceptible de nous parachuter sur des **sites d'arnaque**.

L'objectif d'un tel site est tout simplement de **récolter l'argent des consommateurs** : le client paye pour une commande qui ne lui sera jamais livrée, ou bien il reçoit un produit dont la qualité est bien inférieure à celle qui était promise.

Il serait extrêmement dommage de se priver de cette immense vitrine que représente Internet. Mais pour pouvoir en profiter en toute sérénité, sans risquer de se faire escroquer, il est important de savoir faire la différence entre un site digne de confiance et un site frauduleux.

Les indices qui doivent éveiller votre méfiance

Dans le premier chapitre de ce cours, vous avez pu apprendre qu'afin de ne pas devenir victime d'une tentative de phishing, il est préférable d'éviter de cliquer sur un lien contenu dans un courrier électronique. Il en va de même pour les sites d'arnaque : **ces derniers tentent souvent de vous attirer au moyen d'un lien présent sur un autre site Internet ou sur un forum de discussion**.

> La première précaution à prendre pour ne pas se faire escroquer serait donc de **ne pas faire des achats sur un site auquel vous avez accédé via un lien**.

Une règle qui n'est pas si simple à suivre ! En effet, quand nous comparons des prix sur Internet, de nombreux liens en rapport avec l'objet recherché apparaissent. Et c'est bien souvent grâce à ces liens que nous finissons par dénicher « la » bonne affaire.

> Imaginons par exemple un consommateur à la recherche d'un vélo d'appartement : il consulte les sites de vente d'articles de sport les plus connus et voit apparaître un lien lui proposant le même genre d'articles à des prix défiant toute concurrence. Notre consommateur clique sur ce lien.

La page Internet qui s'affiche à l'écran lui parait parfaitement normale et l'article, proposé à un prix effectivement attractif, correspond en tous points à ce qu'il recherche.

Doit-il considérer qu'il s'agit d'une escroquerie pour la seule raison qu'il a accédé au site en cliquant sur un lien ?

Heureusement, ce consommateur a à sa disposition différents moyens de **vérifier la fiabilité du site**.

L'aspect général du site

Soyez attentif à l'aspect du site Internet visité.

- Les éléments paraissent-ils désordonnés (images non alignées entre elles, textes non centrés, caractères qui débordent...) ?
- La présentation paraît-elle peu soignée ?

Dans ce cas, il y a de fortes chances que ce site ait été conçu par des pirates.

Les fautes d'orthographe

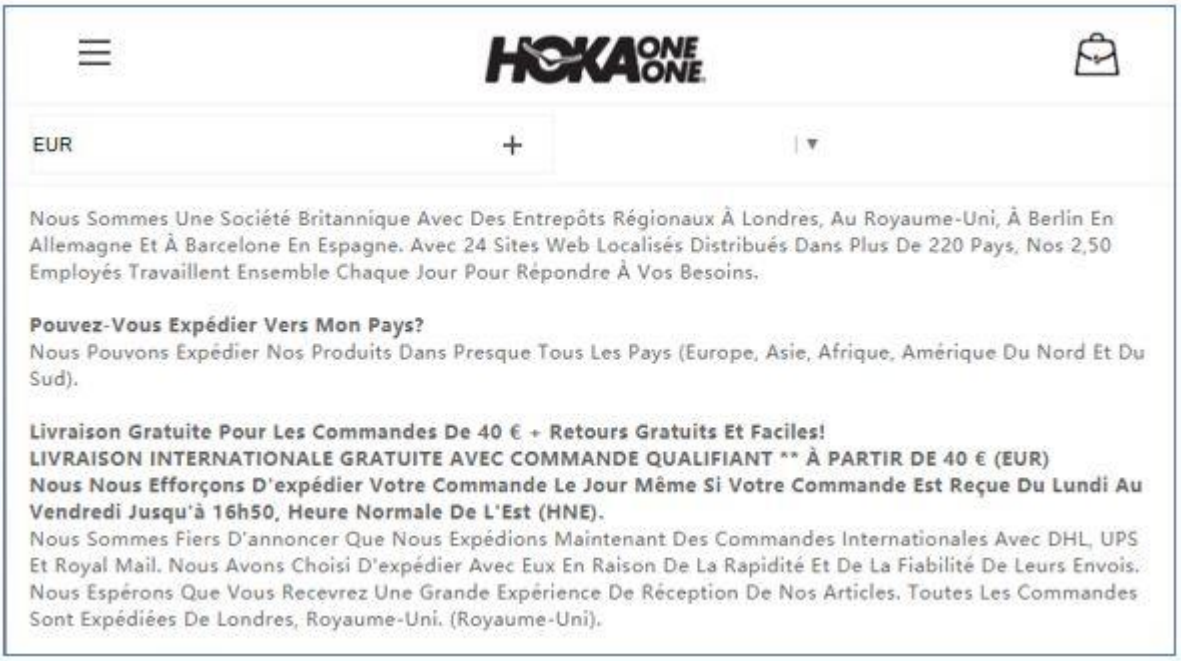
« Nous Espérons Que **Vous Recevrez Une Grande Expérience De Réception** De Nos Articles. »

Cette phrase, extraite d'une page Internet créée par des escrocs, n'est absolument pas correcte d'un point de vue grammatical.

Des fautes d'orthographe, de grammaire ou de syntaxe doivent immédiatement vous alerter : ces indices, assez faciles à repérer, ne laissent pas de place au doute et sont révélateurs d'une tentative d'escroquerie. Comme nous l'avons déjà indiqué précédemment dans ce cours, l'inverse n'est malheureusement pas vrai : l'absence de faute n'est pas à elle seule une garantie suffisante de fiabilité.

Dans l'image ci-dessous, extraite d'un site Internet frauduleux, on peut observer un défaut de présentation : chacun des mots de la page commence en effet par une lettre majuscule.

D'autre part, le texte, bien qu'exempt de fautes d'orthographe, montre une manière de s'exprimer pour le moins inhabituelle : (« *entrepôts régionaux à Londres, Berlin et Barcelone, 24 sites web localisés, Si votre commande est reçue du lundi au vendredi jusqu'à 16h50, heure normale de l'est !* »)



Exemple d'une page Internet suspecte

Des liens qui ne fonctionnent pas

La présence, sur la page, de logos de grandes entreprises comme ceux des réseaux sociaux Facebook (ou Meta) ou Twitter, n’est pas un gage de sérieux. Les pirates utilisent en effet régulièrement ces logos, pensant ainsi donner à leurs sites un caractère véridique. Il est conseillé de cliquer sur ces logos pour vérifier leur véracité.

Reprenons l’exemple de notre consommateur, qui souhaite acheter un vélo d’appartement et qui cherche à vérifier la fiabilité d’un site nommé « *Lesmeilleursprixdusport.com* » ; il clique alors sur le logo Facebook présent sur le site : le lien le mène bien sur une page Facebook, mais malheureusement pas sur celle de l’entreprise !

Un vrai lien doit en effet vous renvoyer sur la page Facebook de l’entreprise concernée ; sans cela, il est factice et indique que le site sur lequel vous vous trouvez n’est pas fiable.

Si les liens ne fonctionnent pas ou s’ils sont factices, vous avez certainement affaire à un site frauduleux.

Référencement du site

Les sites Internet, qu’ils soient fiables ou frauduleux, sont tous référencés sur les moteurs de recherche comme Google. C'est-à-dire qu'ils apparaissent dans les résultats de recherche. La réputation d'un site fait partie des facteurs pris en compte

par Google pour le classement des résultats : ainsi, si un site n'apparaît pas dans les 2/3 premières pages de résultats, vous êtes en droit de douter de sa fiabilité.

D'autre part, la recherche de bonnes affaires ne doit pas vous conduire à accepter sans méfiance des prix trop alléchants : prenez le temps de comparer les prix proposés par la concurrence et soyez **prudent lorsqu'ils sont trop attractifs**.

Contrôlez la fiabilité du site

Mentions légales & conditions générales de vente (CGV)

> Les mentions légales d'un site Internet regroupent un ensemble d'informations devant permettre aux internautes d'identifier le propriétaire (ou responsable) du site Internet qu'ils visitent. Elles sont **obligatoires** pour tous les sites, qu'ils soient professionnels ou personnels, et sont généralement situées tout en bas de chaque page d'un site.

Les mentions légales doivent indiquer les éléments suivants :

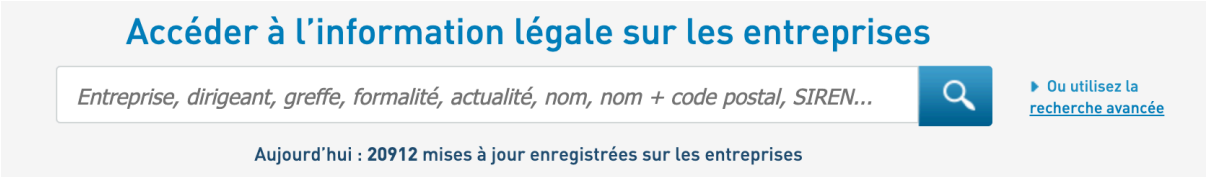
- raison sociale (nom), forme juridique et n° de Siret de l'entreprise ;
- adresse du siège social, adresse de courrier électronique et numéro de téléphone ;
- numéro d'immatriculation au registre du commerce et des sociétés (RCS) et numéro de TVA intracommunautaire ;
- CGV ou conditions générales de vente (pour les sites commerciaux ou sites de vente en ligne uniquement).

> Ne réalisez pas d'achat et ne communiquez aucune information sur un site qui n'en comporterait pas. Leur absence représentant une entorse à la loi, il est fort probable que le site soit frauduleux.

Par exemple, sur ce site Internet proposant des paires de baskets à prix sacrifiés, les mentions légales n'apparaissent nulle part.

À l'inverse, voici le bas de page du site Decathlon.fr, sur lequel les mentions légales sont parfaitement accessibles.

Pour encore plus de sécurité, tout internaute peut noter le n° de Siret de l'entreprise éditrice du site, puis se rendre sur le site Infogreffe.fr. Ce site vous propose de saisir le nom ou le numéro de Siret d'une entreprise, vous permettant ainsi de vérifier son existence, son activité et ses coordonnées.

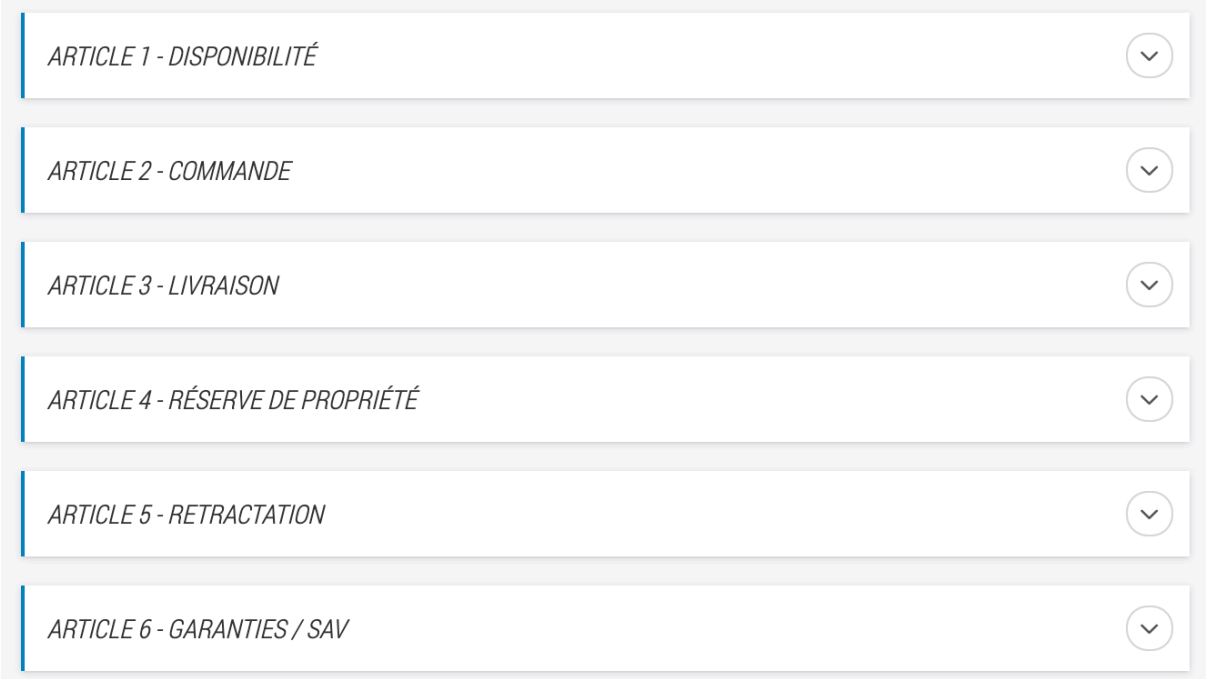


Moteur de recherche sur la page d'accueil du site Infogreffe

Pour les **sites commerciaux**, le site Internet doit préciser les les **CGV** ou **conditions générales de vente** : elles s'affichent généralement sous la forme d'une suite d'articles précisant les modalités de commande et de livraison, ainsi que la politique de retour et de garantie offerte par l'entreprise.

L'absence de CGV est un autre élément indicateur d'une probable fraude.

À titre d'exemple, l'image ci-dessous vous présente un extrait des conditions générales de vente du site Décathlon :



CGV de Décathlon

Le protocole HTTPS

Le terme *HTTP* ou « HyperText Transfer Protocol » correspond à un **protocole de communication** permettant à un ordinateur d'échanger, au moyen d'un navigateur

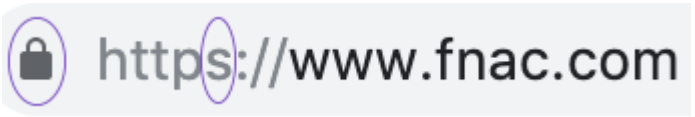
web (comme Google Chrome ou Firefox), avec les serveurs des sites Internet visités.

Pour afficher une page web sur votre écran, votre ordinateur a en effet besoin de recevoir l'information provenant du site Internet visité ; cet échange d'informations serait impossible sans le HTTP. Mais ce protocole **ne permet pas de coder** (ou crypter) les informations échangées entre votre ordinateur et les serveurs des différents sites sur lesquels vous vous rendez. C'est-à-dire qu'un pirate qui intercepterait ces échanges pourrait donc les lire sans difficulté.

Ainsi, a été créé le **protocole HTTPS**. Il fonctionne comme le protocole HTTP, excepté qu'il **permet en outre de crypter** les informations échangées : de cette manière, même si un pirate parvenait à dérober des informations, il serait incapable de les déchiffrer et ne pourrait donc pas les utiliser.

> Si vous souhaitez réaliser des achats sur Internet, il est donc très important de vérifier la sécurité fournie par le site vendeur.

Dans la barre d'adresse en haut de votre navigateur, l'adresse doit commencer par HTTPS (site sécurisé) et non par HTTP (non sécurisé). Si ce n'est pas le cas, il est fortement déconseillé d'effectuer un achat. La grande majorité des sites affichent également un petit cadenas à gauche de la barre d'adresse, pour indiquer à leurs clients que les transactions sont sécurisées.



URL du site commercial de la Fnac

> En effectuant vos achats sur des sites équipés du protocole HTTPS, vous pouvez être **absolument certain que vos données** (comme votre numéro de carte bancaire) ne seront utilisées que par le site dont vous êtes client. Aucun pirate ne sera en mesure de les dérober ou de les exploiter.

En cas de doute : réagissez

Consultez les avis des autres internautes

Supposons maintenant que vous ayez vérifié l'ensemble des éléments cités dans ce chapitre afin de vous assurer de la fiabilité d'un site sur lequel vous aimeriez faire des achats, mais que malgré tout, vous ayez encore des doutes.

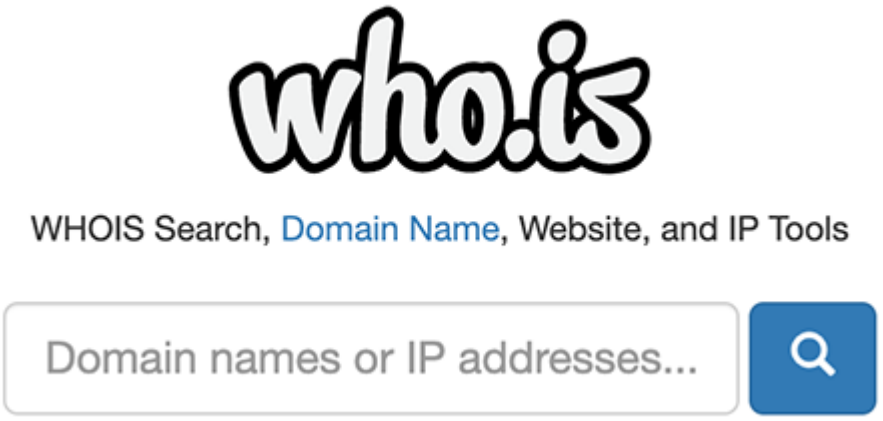
> Vous pouvez alors consulter les avis des autres internautes : il suffit pour cela de taper dans un moteur de recherche le terme « Avis » suivi du nom du site.

Le consommateur à la recherche d'un vélo d'appartement dont je vous parlais au début de ce chapitre a ainsi tapé les mots « *Avis Lesmeilleursprixdusport.com* » sur son moteur de recherche favori et a vu apparaître non pas un, mais plusieurs **avis extrêmement négatifs** qui alertaient les internautes sur la forte probabilité de se faire arnaquer en effectuant un achat sur ce site.

Interrogez « Who is »

Il arrive néanmoins, lorsque le site est peu connu ou s'il s'agit d'une petite entreprise, que vous ne trouviez pas d'avis de clients ou bien que ceux-ci ne vous permettent pas de trancher (que ce soit en sa faveur ou non). Vous pouvez dans ce cas utiliser le site « **Who is** » (« Qui est ? » en français) :

Il s'agit d'un service gratuit permettant de rechercher des informations sur la personne ou l'entreprise responsable d'un site Internet. Pour l'utiliser, tapez simplement l'adresse https://who.is dans votre navigateur puis saisissez le nom du site dont vous voulez vérifier la fiabilité.



Moteur de recherche Who.is sur la page d'accueil du site

Si votre recherche s'avère infructueuse et que *Who is* n'affiche aucun nom, ni coordonnées de contact, lié au site concerné, cela peut être un signe annonciateur de fraude. **D'une manière générale, il est prudent d'éviter toute transaction sur un site inconnu du Who is.**

Que faire si vous repérez un site frauduleux ?

Tout internaute a la possibilité de signaler aux autorités l'existence d'un site frauduleux, en se rendant sur le site **https://www.internet-signalement.gouv.fr** puis en suivant la procédure indiquée.

> Vous ne pouvez cependant pas l'utiliser pour signaler une page Internet qui vous paraît choquante ou immorale. Le site concerné doit afficher un contenu illicite, au sens où il est interdit par la loi française.

Votre signalement sera ensuite étudié par un policier ou gendarme appartenant au PHAROS (plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements), un service dépendant de la police judiciaire.

Outre cette plateforme, il existe un autre moyen de signaler les sites frauduleux : vous pouvez joindre le **service public « Info escroqueries »** en appelant le 0 805 805 817 (du lundi au vendredi de 9h à 18h30), l'appel est gratuit.

> Ce service a également vocation à vous renseigner, et à répondre aux éventuelles questions que vous pourriez vous poser sur ce sujet.

En résumé

Pour repérer un site frauduleux :

- Attention à l'aspect général du site (présentation, fautes de français, liens factices) ;
- Vérifiez la présence du protocole HTTPS ;
- Consultez les avis des autres internautes et interrogez le Who is ;
- Si vous repérez un site frauduleux, signalez-le aux autorités compétentes.

Maîtrisez vos données personnelles et vos informations de navigation

Différenciez données personnelles & informations de navigation

L'article 4 du règlement général sur la protection des données définit les **données à caractère personnel** comme « *toute information se rapportant à une personne physique identifiée ou identifiable* ».

> Autrement dit, toute donnée liée à votre identité, comme votre identifiant, votre nom, votre date de naissance, votre adresse e-mail ou encore vos données de localisation (adresse postale, adresse IP), etc.

Quant aux **données de navigation**, elles correspondent à votre comportement sur le web : elles enregistrent en effet votre parcours lorsque vous êtes connecté, et mémorisent ainsi les liens sur lesquels vous cliquez et les sites que vous visitez.

> Les données de navigation sont donc propres à chacun et en cela, elles font partie des données personnelles.

C'est en associant données personnelles et données de navigation que les sites Internet sont en mesure d'afficher des publicités personnalisées (adaptées à vos centres d'intérêt et à vos goûts) sur les pages que vous visitez.

> Comment les sites Internet collectent-ils toutes ces données ? Grâce aux cookies ! 🍪

Les cookies

> Lorsque vous vous rendez pour la première fois sur un site Internet, ce dernier dépose un cookie dans le disque dur de votre ordinateur : c'est un petit fichier destiné à enregistrer vos données personnelles et de navigation.

> Supposons que vous ayez besoin de créer un compte client sur un site de vente en ligne ; lors de la création de votre compte, vous choisissez vos identifiant et mot de passe. Si vous revenez sur ce site quelques jours plus tard, il ne sera pas nécessaire de saisir de nouveau ces informations : le site accèdera au cookie qu'il a stocké dans votre ordinateur et récupèrera les informations qui y sont enregistrées (telles vos identifiant et mot de passe) pour remplir les champs à votre place.

Selon la loi, le site qui dépose ces cookies sur votre disque dur doit les supprimer au bout d'un an (13 mois exactement) ; dans la réalité, la plupart restent sur votre disque dur jusqu'à ce que vous les supprimiez. On les appelle les **cookies *permanents***.

De même, lorsque vous ajoutez des articles à votre panier, si vous continuez à visiter le site web en question et que vous vous rendez plus tard sur la page de panier, celui-ci contient toujours les articles choisis précédemment : le cookie les a enregistrés, afin de vous éviter d'avoir à les chercher de nouveau.

On parle ici de ***cookie de session*** : ces cookies ne demeurent que temporairement sur votre ordinateur et sont supprimés dès que vous quittez le site.

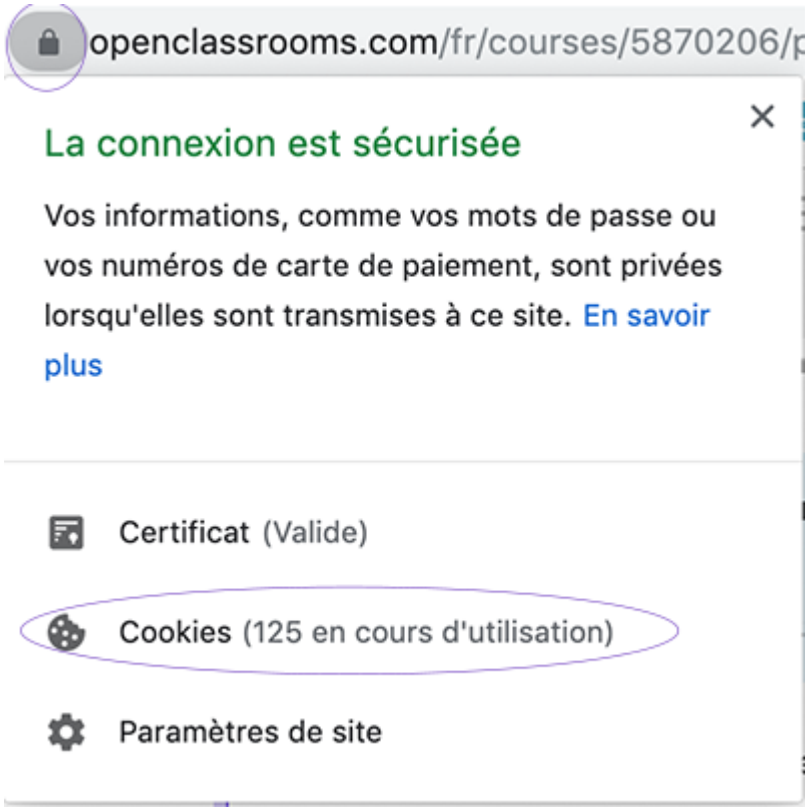
Qu'ils soient ou non permanents, en conservant certaines données, ces cookies permettent donc de faciliter votre identification et votre navigation.

Il s'agit dans ce cas de **cookies internes** (on rencontre aussi parfois le terme de cookie *propriétaire*) ; leur rôle est de garantir le bon fonctionnement du site concerné.

Un cookie ne peut être lu et utilisé que par le site qui l'a déposé. Il est donc **impossible de l'utiliser à des fins malveillantes** (comme dérober des données sur votre disque dur ou installer un virus sur votre machine).

Les cookies étant gérés par votre navigateur Internet, c'est en paramétrant ce dernier que vous pouvez accepter ou refuser les cookies.

Selon le navigateur Internet que vous utilisez, vous pourrez facilement **prendre connaissance du nombre de cookies** déposés sur votre ordinateur. Dans *Google Chrome* par exemple, il suffit de cliquer, dans la barre d'adresse, sur le petit cadenas à gauche de l'URL du site :



Menu d'accès pour paramétrer vos cookies sur Google Chrome

Les **cookies tiers** constituent donc une puissante source de renseignements, qui seront ensuite utilisés à des **fins publicitaires**. Il arrive ainsi que sur certains sites, plusieurs dizaines de cookies tiers soient déposés sur l'ordinateur du visiteur.

Bloquer les cookies internes

Il est possible de refuser les cookies internes ; ce n'est **toutefois pas recommandé**. Ce type de cookies n'a en effet qu'un seul objectif : celui de faciliter votre navigation sur Internet. En cas de refus, certains sites pourront ne plus fonctionner correctement ; quelques-uns pourront même devenir totalement inaccessibles.

Lorsque vous visitez un site, une phrase similaire à celle de l'image ci-dessous apparaît généralement en bas de votre écran :

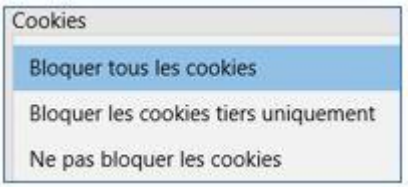
Exemple d'une demande d'acceptation des cookies sur le site Le Monde.fr

Par défaut, les cookies sont acceptés par les navigateurs Internet.

Si vous souhaitez bloquer les cookies pour l'ensemble des sites que vous visitez, suivez la procédure correspondante à votre navigateur :

Microsoft Edge

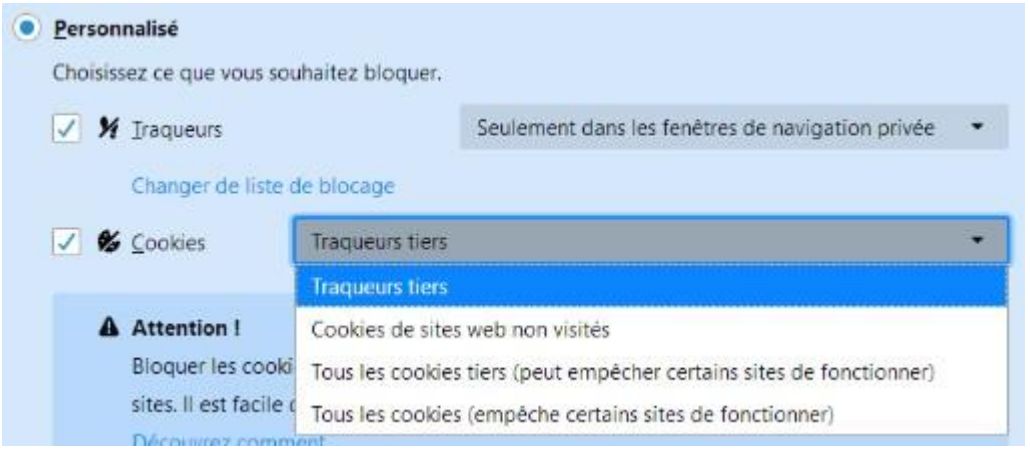
1. Cliquez sur le bouton **Paramètres** ··· en haut à droite de l'écran.
2. Cliquez sur **Paramètres**.
3. Cliquez sur **Afficher les paramètres avancés**.
4. Choisissez de **bloquer** ou non **les cookies**.



Firefox

Cliquez sur le bouton Options ☰ puis sur **Blocage de contenu**.

1. Sélectionnez **Personnalisé**



2. Cochez la case devant **Cookies**.
3. Choisissez ***Tous les cookies*** pour bloquer tout type de cookies, quel que soit le site visité.
4. **Fermez la page** : les modifications sont automatiquement enregistrées.

Chrome

1. Cliquez sur le bouton Options ⋮ en haut à droite de l'écran.
2. Cliquez sur **Paramètres**.
3. À gauche, cliquez sur **Paramètres avancés** puis sur **Confidentialité & sécurité**.
4. À droite, cliquez sur **Paramètres du site** puis sur **Cookies**.
5. Pour bloquer tous les cookies, désactivez l'option : « *Autoriser les sites à enregistrer et à lire les données des cookies (recommandé)* ».

Safari

1. Cliquez dans la barre de menus sur **Préférences** puis sur **Confidentialité**.

2. Sélectionnez « Bloquer tous les cookies ».

Supprimer les cookies de son navigateur

Supposons qu'afin de faciliter votre navigation, vous ayez décidé d'accepter les cookies. Sachez que vous pouvez procéder ponctuellement à la **suppression des cookies**.

Cela ne veut pas dire que vous les refusez.

Prenons l'exemple d'un consommateur qui recherche une table basse sur Le Bon Coin. Supposons qu'il ait supprimé les cookies sur son ordinateur et qu'il souhaite cette fois faire l'acquisition d'un nouveau canapé : il se connecte donc à nouveau sur Le Bon coin.
Comme le cookie qui contenait ses informations de connexion a été supprimé, il doit saisir lui-même ses identifiant et mot de passe, comme lors de sa toute première connexion.

Mais comme les cookies ne sont pas bloqués, le site en dépose un nouveau sur son disque dur (et pourra ainsi préremplir les champs lors d'une prochaine visite).

Vous pouvez donc choisir de supprimer les cookies pour certains sites seulement, ou pour tous les sites que vous visitez. Cela permet également de libérer de l'espace sur votre disque dur.

Pour supprimer les cookies, suivez la procédure correspondant à votre navigateur :

Microsoft Edge

1. Cliquez sur le bouton Paramètres  en haut à droite de l'écran puis sur **Paramètres**.
2. Dans la rubrique **Effacer les données de navigation**, cliquez sur **Choisir les éléments à effacer**.
3. Cochez la case **Cookies et données de sites web enregistrées** puis cliquez sur **Effacer**.

Firefox

1. Cliquez sur le bouton Options  puis sur **Options**.
2. Sélectionnez le panneau **Vie privée et sécurité**.

1. Cliquez sur le bouton **Gérer les données** de la section **Cookies et données de sites**.
2. Pour supprimer les cookies de l'ensemble des sites, cliquez sur le bouton **Supprimer les sites affichés**.
3. Cliquez sur **Enregistrer les changements**.

Chrome

1. Cliquez sur le bouton Options en haut à droite de l'écran : ⋮
2. Cliquez sur **Paramètres**.
3. À gauche, cliquez sur **Paramètres avancés** puis sur **Confidentialité & sécurité**.
4. À droite, cliquez sur **Paramètres du site** puis sur **Cookies**.
5. Cliquez ensuite sur **Afficher l'ensemble des cookies et données de site**.
6. Cliquez sur le bouton **Tout supprimer**.

Safari

1. Cliquez dans la barre de menus sur **Préférences** puis sur **Confidentialité**.
2. Cliquez sur le bouton **Afficher les cookies**.
3. Cliquez sur **Supprimer toutes les données de navigation**.

Limitez les traces de votre navigation sur le web

Supprimez tout ou partie des données de navigation

Pour protéger votre vie privée, il est recommandé d'effacer régulièrement vos données de navigation. Vous pouvez choisir de supprimer les données liées à certains sites seulement, ou bien celles de tous les sites visités.

En outre, tout comme la suppression des cookies, celles des données de navigation permet de **libérer de l'espace sur votre disque dur**. Bien souvent, elles encombrent l'espace de stockage de votre machine et ralentissent son fonctionnement.

Comment supprimer mes données de navigation ?

Microsoft Edge

1. Cliquez sur le bouton Paramètres ··· en haut à droite de l'écran puis sur **Paramètres**.
2. Dans la rubrique **Effacer les données de navigation**, cliquez sur **Choisir les éléments à effacer**.
3. Cochez la case **Historique de navigation** et **Données de formulaire** puis cliquez sur **Effacer**.

Firefox

1. Cliquez sur le bouton Options ☰ puis sur **Options**.
2. Sélectionnez le panneau **Vie privée et sécurité** puis cliquez sur le bouton **Effacer les données** de la section **Cookies et données de sites**.

Chrome

1. Cliquez sur le bouton Options ⋮ en haut à droite de l'écran.
2. Cliquez sur **Paramètres**.
3. À gauche, cliquez sur **Paramètres avancés** puis sur **Confidentialité & sécurité**.
4. Cliquez sur **Effacer les données de navigation** puis sur **Effacer les données**.

Safari

1. Cliquez dans la barre de menus sur **Historique** puis sur **Effacer l'historique**.
2. Cliquez sur le **menu local** & indiquez la **période** pour laquelle vous voulez effacer l'historique.

Utilisez les paramètres de confidentialité de votre navigateur Internet

Quel que soit le navigateur Internet que vous utilisez, vous avez la possibilité de **personnaliser les paramètres de confidentialité**.

Le fait d'accepter ou non les cookies, leur suppression, tout comme l'effacement des données de navigation, font partie de ces paramètres.

Ces derniers vous permettent également de bloquer ou de restreindre certains sites Internet et pas d'autres : si vous pouvez sans crainte faire confiance à certains sites (comme par exemple les sites bancaires ou le site des impôts), il est prudent, à l'inverse, de vous méfier d'autres sites moins sécurisés, et de vouloir restreindre ou bloquer les autorisations d'accès de ces sites.

Les paramètres de confidentialité des navigateurs vous permettent de décider :

- le temps de stockage des cookies sur votre ordinateur avant leur suppression ;
- de garder ou non la saisie semi-automatique des recherches et des adresses ;
- de donner ou non votre accord pour envoyer les adresses des pages que vous consultez au moteur de recherches, et de donner ou non votre accord pour des fins de statistiques.
  - Sur **Firefox**, utilisez le menu *Vie privée.*
  - Sur **Chrome, la** rubrique *Paramètres de site.*
  - Sur **Microsoft Edge**, la rubrique *Paramètres.*

Bloquez les cookies tiers

Il existe également les **cookies tiers** ; ces derniers ne sont pas déposés sur votre ordinateur par le site que vous visitez, mais par des tiers : des sites partenaires de celui qui vous intéresse.

Ils collectent davantage d'informations : votre cheminement sur Internet (les sites, pages et sous-pages visités, et le temps passé sur chacune) les intéresse particulièrement, mais aussi vos données personnelles, comme l'origine, le sexe ou l'âge.

Reprenons l'exemple du consommateur qui recherche une table basse sur Le Bon coin : lors de sa prochaine visite sur le site, ce consommateur verra probablement apparaître sur sa page Internet des encarts publicitaires pour des sites de vente de mobilier. Cet affichage est rendu possible par l'action des cookies tiers, qui n'ont pas été déposés par Le Bon Coin, mais par des sites partenaires de ce dernier.

Ces cookies ne permettent pas d'améliorer votre navigation et ne sont pas nécessaires pour profiter pleinement d'Internet.

Par conséquent, si vous souhaitez **protéger votre vie privée et limiter les traces** de votre navigation sur Internet, il est recommandé de les **refuser par défaut**.

> Vous pouvez les refuser, mais les cela ne permet malheureusement pas à un internaute d'éviter toute publicité ! En effet, vous verrez autant de publicités que si vous les acceptez ; mais elles ne seront tout simplement plus adaptées à vos goûts et centres d'intérêt.

Quel que soit le navigateur que vous utilisez, il permet le blocage des cookies tiers : référez-vous pour cela au paragraphe : « Accepter ou refuser les cookies ».

La procédure pour bloquer les cookies tiers est en effet la même que pour accepter ou refuser les cookies internes. À la fin de la manipulation, vous sélectionnerez simplement l'option « *Bloquer les cookies tiers* » et non « *Bloquer les cookies* ».

Empêchez l'installation des traqueurs

> Une grande partie des sites Internet suivent votre cheminement sur la toile : de la première à la dernière page visitée, en passant par les liens empruntés et les recherches effectuées, les « traqueurs » enregistrent constamment votre activité : c'est ce que l'on appelle le « pistage ».

Les cookies tiers font ainsi partie des traqueurs. Mais **bloquer ces derniers n'est pas suffisant pour éviter d'être pisté**.

Il existe en effet des traqueurs d'autres sortes : certains contenus de sites ou scripts* continueront de vous suivre, même si vous refusez les cookies tiers.

> Qu'est-ce qu'un script ?

Un script est un programme chargé d'exécuter une action précise au moment de l'affichage d'une page web, ou lorsqu'un utilisateur réalise une action.

Il est toutefois **possible de refuser d'être pisté**. Sachez que l'activation de cette fonctionnalité ne perturbera en rien votre navigation. La procédure à suivre diffère là encore selon le navigateur que vous utilisez :

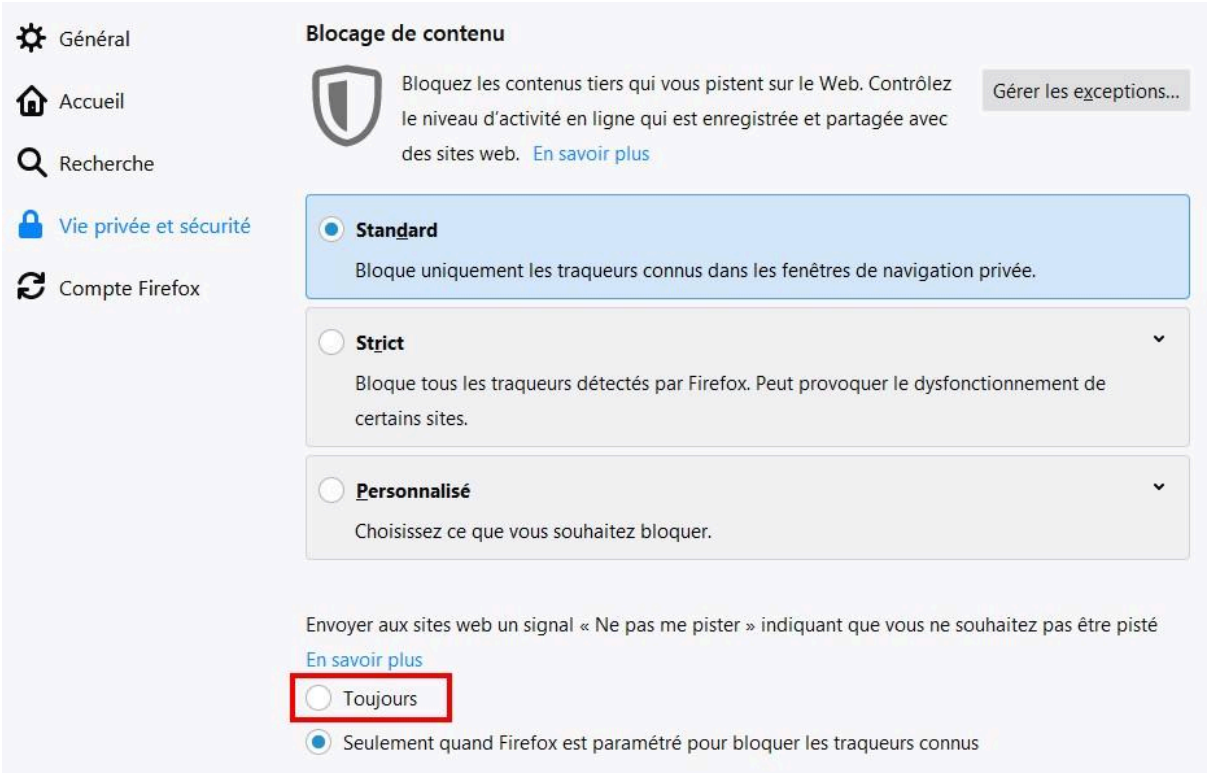
Microsoft Edge

1. Cliquez sur le bouton Paramètres  en haut à droite de l'écran puis sur **Paramètres**.
2. Cliquez sur **Paramètres avancés**.
3. Activez l'option **Envoyer des demandes Do Not Track**.

Firefox

1. Cliquez sur le bouton Options  puis sur **Blocage de contenu**.

2. Sous *Envoyer aux sites web un signal « Ne pas me pister » indiquant que vous ne souhaitez pas être pisté*, choisissez **Toujours**.



3. Fermez la page. Les modifications seront enregistrées automatiquement.

Chrome

1. Cliquez sur le bouton Options ⋮ en haut à droite de l'écran.
2. Cliquez sur **Paramètres**.
3. À gauche, cliquez sur **Paramètres avancés** puis sur **Confidentialité & sécurité**.
4. Activez l'option ***Envoyer une demande "Interdire le suivi" pendant la navigation***.

Safari (selon version)

Ne soyez pas étonné si vous ne trouvez pas l'option ***Ne pas me suivre*** dans **Safari** : en activant cette option, vous indiquez aux sites Internet votre souhait de ne pas être pisté. Or, selon la loi, même si vous exprimez ce souhait, les publicitaires ont tout de même le droit de vous suivre !

Certains publicitaires feront le choix de respecter votre volonté mais ils n'y sont absolument pas obligés: ils peuvent donc continuer de vous traquer en toute légalité ! Cette option étant basée sur le volontariat des entreprises publicitaires, Apple a jugé qu'elle n'avait que peu d'intérêt et l'a retirée de la dernière version de son navigateur.

Si votre version de Safari vous le permet :

1. Cliquez dans la barre de menus sur **Préférences** puis sur **Confidentialité**.
2. Cochez la case ***Demander aux sites web de ne pas me suivre***.

En résumé

- Les cookies sont de petits fichiers destinés à enregistrer vos données personnelles et de navigation.
-
- Pour limiter les traces de votre navigation et ainsi protéger votre vie privée, utilisez les paramètres de votre navigateur pour :
    - accepter ou refuser les cookies ;
    - effacer vos données de navigation ;
    - choisir votre niveau de confidentialité ;
    - bloquer les cookies tiers ;
    - demander aux sites volontaires de ne pas vous pister.

Utilisez des mots de passe robustes

Que ce soit pour consulter notre compte bancaire ou notre messagerie électronique, ou encore pour effectuer une démarche administrative, nous nous connectons très souvent sur des sites Internet. Pour accéder à nos comptes, nous sommes nombreux à utiliser des **mots de passe trop simples** ou bien à utiliser un **mot de passe identique** pour l'ensemble de nos comptes, quand ce n'est pas les deux à la fois !

Or, en pensant ainsi faciliter notre quotidien, nous mettons en péril notre sécurité.

Les mots de passe (qu'ils aient été trop simples à deviner ou qu'ils aient été dérobés) sont responsables de près de 80 % des actes de piratage. Il est donc essentiel de connaître les règles et précautions relatives à leur bon usage.

Adoptez les bons réflexes

Utilisez un mot de passe unique pour chaque compte ou service

De prime abord, mémoriser un **unique mot de passe** semble être la solution la plus simple et la plus pratique ! C'est pourtant une **méthode risquée** que vous devrez absolument éviter... car un pirate qui réussirait à accéder à l'un de vos comptes aurait automatiquement accès à tous les autres.

C'est ce que l'on appelle un « **piratage en cascade** ».

Imaginez que le code de votre carte bancaire soit le même que le code de déverrouillage de votre smartphone… cela serait extrêmement risqué !

Il est donc essentiel d'utiliser des **mots de passe distincts** pour chacun de vos comptes en ligne.

Choisissez un mot de passe sans lien avec votre identité

Selon une étude réalisée par un étudiant diplômé de l'Université de Colombie-Britannique, un piratage sur 5 est l'œuvre d'une personne de notre entourage.

Les piratages commis par des proches sont donc plus courants qu'on ne le croit ; or, ces derniers essaieront tout naturellement de déduire votre mot de passe à partir de ce qu'ils connaissent de vous, comme les prénoms de vos enfants ou celui de votre chanteur préféré, votre date ou lieu de naissance, ou encore l'endroit où vous aimez

passer vos vacances.

Quand bien même auriez-vous en vos proches une confiance absolue, les noms, dates de naissance et autres éléments découlant de votre identité, s'ils sont faciles à mémoriser, peuvent facilement être découverts en ligne.

Tout ce qui découle de votre identité doit donc être évité.

Cette précaution prévaut aussi pour la **fameuse « question secrète »**, une option proposée par de nombreux services, à laquelle vous devez répondre afin de prouver votre identité en cas d'oubli du mot de passe : évitez de choisir une réponse qui pourra facilement être trouvée par un proche ou découverte sur Internet (comme le nom de jeune fille de votre mère ou le lieu de naissance de votre père) : **utilisez plutôt une information que vous êtes seul à connaître**.

Modifiez systématiquement et au plus tôt les mots de passe par défaut

De nombreux services vous attribuent un mot de passe « par défaut » : lors de votre inscription à un service en ligne ou lors de la création de votre espace client, la plupart des sites vous envoient un mail afin de vous transmettre un mot de passe, composé de manière aléatoire par un « générateur de mot de passe ».

Les mots de passe communiqués par e-mail présentent un **risque de piratage accru**, l'e-mail étant susceptible d'être intercepté par un pirate, qui aurait alors immédiatement accès à votre compte.

Pour mieux vous protéger, connectez-vous au compte concerné en utilisant le mot de passe fourni par défaut et **modifiez-le dès votre première connexion** par un autre que vous aurez composé vous-même.

De manière générale, il est conseillé de ne jamais envoyer de courriel contenant ses mots de passe.

Activez la double authentification

Lorsque cela est possible, activez la **double authentification**. Cette option permet de **contrôler votre identité par 2 moyens différents** avant d'autoriser l'accès à votre compte : en tant qu'utilisateur, vous devez non seulement connaître votre mot de passe, mais également être capable de taper un code à usage unique, le plus souvent transmis par SMS. Ainsi, même en cas de piratage de votre mot de passe, l'accès à vos données demeurera impossible.

Quasiment tous les systèmes de banque en ligne utilisent la double authentification pour valider les paiements réalisés sur Internet. **Cette fonctionnalité fournit une très forte sécurité**.

Respectez quelques précautions essentielles

Les mots de passe à éviter

Durant les 5 dernières années, les 2 mots de passe les plus utilisés ont été « *123456* » et «*password*» ("motdepasse"). « *Azerty* », « *Iloveyou* » ou encore « *Football* » sont également des choix très fréquents... mais ils n'apportent aucune sécurité !

En cas de tentative de piratage, les mots de passe les plus courants sont les premiers à être testés. Les pirates utilisent pour cela des **logiciels spécialisés**, capables de tester l'un après l'autre tous les mots du dictionnaire, y compris les noms propres, ainsi que les expressions courantes et mots de passe les plus connus.

Sont à proscrire absolument :

- les **mots du langage courant** courant comme « *motdepasse* » ou « *licorne* » 🦄 ;
- les **suites logiques** de chiffres et de lettres comme « *123456789* » ou « *Qwerty123456* » ;
- les **expressions simples**, **citations** ou phrases toutes faites (**proverbes** par exemple) ; même exprimées phonétiquement, telles que « *1tienvomeixque2tul'auras* ».

Votre mot de passe doit être impossible à deviner, même par l'un de vos proches.

Par exemple, si vous êtes l'heureux parent d'une fille prénommée **Julie** et née le **22 juin**, vous éviterez ***Julie2206***. 

Les pirates informatiques testent également les **noms de célébrités**, qu'il s'agisse d'acteurs, chanteurs, animateurs ou encore équipes sportives, tous sont également à proscrire.

Certains logiciels utilisés par les pirates sont capables de tester toutes les combinaisons de caractères possibles. Ces tentatives de piratage sont nommées « **attaques par force brute** ».

Ainsi, plus le nombre de caractères du mot de passe est élevé, plus il faudra de temps à un tel programme pour découvrir la bonne combinaison. Pour cette même raison, vous devrez, pour créer un mot de passe performant :

- combiner lettres **minuscules et majuscules** avec des **chiffres** et des **caractères spéciaux**.
- choisissez toujours un mot de passe dont le nombre de caractères est **supérieur ou égal à 8**.

Pour découvrir un mot de passe de 10 caractères composé uniquement de lettres minuscules, il faudra à un logiciel spécialisé 26 exposant 10 essais, tandis qu'il lui en faudra 36 exposant 10 si le mot de passe mélange lettres minuscules et chiffres, et 62 exposant 10 s'il est composé à la fois de minuscules, majuscules et chiffres.

Par exemple : « **#Cm,j'aa5op10E.** » serait un excellent mot de passe !

La « **force** » d'un mot de passe, que l'on définit comme sa capacité à résister à une attaque par énumération de toutes les combinaisons possibles, augmente proportionnellement à sa longueur : plus un mot de passe est long, plus le nombre de combinaisons possibles entre les caractères qui le composent est élevé.

Renouvelez vos mots de passe

Contrairement à une croyance largement répandue, le fait de modifier régulièrement vos mots de passe **n'améliore pas votre sécurité**.

En effet, lorsque nous sommes contraints à changer nos mots de passe, nous avons tendance soit à choisir des mots de passe plus faciles à mémoriser que les anciens (et donc plus faibles d'un point de vue sécuritaire), soit à réutiliser les précédents en y apportant seulement un léger changement : « **#Cm,j'aa5op10** » deviendra par exemple « ***Cm,j'aa10op5** ».

Or, une telle modification n'augmente en rien la force de votre mot de passe et ne fait que vous compliquer la tâche (vous risquez ensuite de vous « mélanger les pinceaux », ne sachant plus quelle est la bonne version).

Dans ce cas, quand et pour quelle raison dois-je modifier mes mots de passe ?

Premièrement : s'ils sont trop faibles et ne respectent pas les règles de base d'hygiène numérique (vous les apprendrez dans la dernière partie de ce cours), il est primordial de les modifier.

Deuxièmement : en cas de piratage d'un service sur lequel vous possédez un compte client.

En 2012, le réseau *LinkedIn* a été victime d'une attaque à l'issue de laquelle des pirates ont récupéré plus de 167 millions de mots de passe ! Si vous avez

connaissance d'un tel événement concernant un service dont vous êtes utilisateur, vous devez modifier le mot de passe utilisé le plus rapidement possible.

Veillez à l'endroit où vous stockez vos mots de passe

Il est tentant d'enregistrer vos mots de passe dans un fichier sur votre **ordinateur**, ou dans le bloc-notes de votre **smartphone**, mais ils ne sont malheureusement pas conçus pour cela et ne vous offrent par conséquent aucune sécurité en matière de stockage.

Les pirates commencent généralement par parcourir le contenu de votre ordinateur à la recherche de fichiers du type "*mdp.txt*", "*password.txt*" ou encore « *code.doc* ».

Ne notez pas non plus vos mots de passe dans un e-mail : votre messagerie n'est pas destinée à la protection des données sensibles et elle demeure vulnérable aux attaques.

Il est bien entendu possible de les inscrire sur un papier ou un **carnet** auquel vous seul aurez accès mais là encore, le **risque** existe : vous pouvez vous faire voler votre portefeuille (en supposant que ledit papier y soit rangé), perdre le carnet, ou l'un de vos proches peut un jour en prendre connaissance.

Idéalement, les mots de passe ne devraient donc jamais être écrits quelque part.

Pour les stocker, il est préférable d'utiliser un **gestionnaire de mots de passe**.
Il s'agit d'un **logiciel qui sauvegarde** l'ensemble de vos mots de passe ; vous n'avez alors plus qu'à **retenir un unique mot de passe** dit « *mot de passe maître* » qui vous permet d'accéder au gestionnaire. Une fois déverrouillé, celui-ci se chargera de préremplir pour vous les champs « identifiant » et « mots de passe » de tous les sites sur lesquels vous êtes inscrits, qu'il s'agisse de votre messagerie, d'un réseau social, de votre compte Ameli ou de n'importe quel autre service.

Le mot de passe « maître » protège tous vos autres codes d'accès.

Les gestionnaires de mots de passe sont spécialement conçus pour la protection de vos données et vous offrent une sécurité maximale (leurs méthodes de cryptage sont les mêmes que celles utilisées par les banques) ; l'ANSSI (Agence nationale de sécurité des systèmes d'information) conseille d'ailleurs aux internautes l'utilisation du logiciel gratuit *KeePass*.

N'enregistrez pas vos mots de passe dans votre navigateur

Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis (ne cochez pas la case « *se souvenir du mot de passe* ; ne cliquez pas non plus sur « *Enregistrer* »).

Bien que tentante car fort pratique, cette méthode ne garantit pas votre sécurité :

- **tous les navigateurs ne stockent pas les mots de passe de manière chiffrée** (certains se contentent de les stocker « en clair », les rendant ainsi vulnérables à une attaque) ;
- si d'autres personnes que vous utilisent la même machine, elles pourraient avoir facilement accès à l'ensemble de vos comptes, puisque le navigateur se chargera d'inscrire vos codes d'accès à votre place.

Créez simplement vos mots de passe

Voici une première règle simple, recommandé par l'ANSSI : choisissez des mots de passe d'au moins **12 caractères de différents types** (majuscules, minuscules, chiffres, caractères spéciaux).

Et voici d'autres méthodes reconnues pour vous aider à créer des mots de passe forts et facilement mémorisables, reste à choisir celle qui vous conviendra le mieux !

La méthode phonétique

Choisissez une phrase facile à retenir que vous écrivez phonétiquement : par exemple,« J'ai *acheté huit CD pour cent euros cet après-midi »* deviendra « *ght8CD%E7am* » ou bien « *J'ai écrit 300 pages de texte* » qui donnera « *Gécri300paj2txt* »

La méthode des premières lettres

Elle consiste à ne **conserver que les premières lettres de chaque mot** d'une phrase ; choisissez de préférence une phrase contenant des chiffres et suivez ces quelques règles :

- conservez uniquement la première lettre de chaque mot ;
- conservez la ponctuation et remplacez les chiffres par des nombres (*Un par 1*) ;
- mettez une majuscule si le mot est un nom commun ou un nom propre et une minuscule pour tout autre terme.

Prenons l'exemple de la phrase « ***J'a**pprends **f**acilement **s**ur **l**e **s**ite **O**penClassRooms.**c**om* » : avec la méthode des premières lettres, elle deviendra : « *j'afslSO.c* ».

Comptez le nombre de mots de la phrase et augmentez encore la force du mot de passe en ajoutant un chiffre : « *j'afslSO.c**7*** ».

Enfin, terminez en encadrant votre mot de passe avec des caractères spéciaux : « **j'afslSO.c7** ».

Méthode de la phrase entière

Choisissez une phrase assez simple dont vous vous souviendrez aisément et créez votre mot de passe en tapant entièrement la phrase, sans espace.

Les phrases complètes comportent en effet un nombre si élevé de caractères qu'elles permettent la création de mots de passe extrêmement sûrs.

Par exemple, « ***Jesuis3courssurOpenClassRooms.com*** » est un mot de passe de plus de 30 caractères, mélangeant minuscules, majuscules et chiffres : il offre donc une excellente sécurité tout en étant facile à mémoriser.

La « méthode XKCD »

On l'appelle aussi la **méthode des 4 mots** *(selon l'auteur de Comics Randall Munroe)*

Elle consiste à **associer 4 mots de votre choix**, sans lien les uns avec les autres, en utilisant une majuscule comme première lettre de chaque mot.

Un tel mot de passe comporte un nombre élevé de caractères et l'efficacité est renforcée par le fait que les mots choisis n'ont aucun sens une fois accolés les uns aux autres.

Un mot de passe tel que « ***CoursAspirateurApprendreSoleil*** *»* ou bien « ***SécuritéCanapéCourirGirafe*** *»* vous protègera tout autant que « ****j'afslSO.c7**** ».

Créez votre propre méthode

S'il est déconseillé d'utiliser un mot de passe lié à votre identité, vous pouvez toutefois utiliser des éléments personnels afin de créer un mot de passe. *V*ous obtiendrez ainsi un mot de passe fort, à la fois résistant aux attaques et facile à mémoriser.

Prenons quelques exemples :

Julie est née à ***Ang****ers (4****9****)*, elle vit à ***Mon****tpellier (3****4****)* et part chaque année en vacances à ***Bia****rritz (6****4****)* : elle utilise les **3 premières lettres de chaque ville** puis le **dernier chiffre de chaque département**, en séparant lettres et chiffres par un **dièse (#)**, et en utilisant des majuscules pour la première lettre de chaque ville.

Ce qui nous donne : ***AngMonBia#944***

Arthur a 3 fils : **Bap**tiste, né en 20**07**, **Jul**es, né en 20**09** et **Luc**as, né en 20**12**.
Il a créé son mot de passe en associant les 3 premières lettres des prénoms de ses enfants avec les 2 derniers chiffres de leur année de naissance ; Il utilise une majuscule pour la 1re lettre de chaque prénom et un astérisque après chaque combinaison.

Voici le mot de passe obtenu : ***Bap07*Jul09*Luc12***

Différenciez vos mots de passe

> Sans l'utilisation d'un gestionnaire de mots de passe, comment mémoriser tous les mots de passe complexes et uniques ?

Voici une petite astuce : le principe consiste à créer votre mot de passe en utilisant une partie constante et une seconde partie qui variera en fonction du service utilisé :

« J'ai écrit 300 pages de texte » qui se transforme en « Gécri300paj2txt » (suivant la méthode phonétique) pourra se décliner en :

- *« J'ai écrit 30*0 pages de de texte **sur Facebook** » **«** Gécri300paj2txt**sF** »,
- « J'ai écrit 300 pages de texte **sur Ameli** » « Gécri300paj2txt***s*A** »,
- etc.

« ***J'a**pprends **f**acilement **s**ur **l**e **s**ite **OpenClassRooms.com »*** qui donne **j'afslS**O**.c7** (selon la méthode des premières lettres) peut devenir :

- « ***J'a**pprends **f**acilement **s**ur **l**e **s**ite **Facebook.c**om* » (*j'afslS**F**.c7*)
- « ***J'a**pprends **f**acilement **s**ur **l**e **s**ite **Gmail.c**om » (*« *j'afslS**G**.c7* »)

« *Jesuis3courssur**OpenClassRooms**.com* » issu de la méthode de la phrase entière, est tout aussi simple à adapter à différents sites :

- « *Jesuis3courssur**Facebook**.com* »
- « *Jesuis3courssur**Amazon**.com* ».

Enfin, si vous préférez la méthode XKCD, il vous suffira de remplacer l'un des 4 mots choisis par le nom du site auquel vous désirez vous connecter :

- *CanapéCourirGirafe**Allocations*** pour le site de la CAF
- *CanapéCourirGirafe**Banque*** pour l'accès à votre banque en ligne.

En résumé

- Ne pas utiliser de mot de passe trop simple ou trop répandu, ni de mot de passe directement lié à votre identité.
- Utiliser un mot de passe différent pour chaque service.

- Modifier systématiquement les mots de passe attribués par défaut.
- Ne notez pas vos mots de passe.
- N'enregistrez pas vos mots de passe dans votre navigateur.
- Choisissez un mot de passe d’au moins 12 caractères de différents types en suivant l’une des méthodes suivantes : méthode phonétique, méthode des premières lettres, méthode de la phrase entière ou méthode des 4 mots (vous pouvez également vous en inspirer pour créer votre propre méthode !).

Protégez votre vie privée en ligne

Soyez vigilant à l’usurpation d’identité

Parallèlement au développement d’Internet et des réseaux sociaux, de nouveaux dangers sont apparus, parmi lesquels l’usurpation d’identité.

L’usurpation d’identité consiste à utiliser vos données personnelles ou tout élément permettant de vous identifier, sans vous avoir demandé votre accord au préalable.

Prenons un exemple :

Imaginez qu’un usurpateur publie sur Internet une annonce de location d’appartement.
Lorsqu’un internaute intéressé par l’offre répond à son annonce, l'usurpateur lui explique qu’avant de programmer une visite, il est indispensable de constituer un dossier de candidature. Il lui demande pour cela de lui communiquer une pièce d’identité, un justificatif de domicile et un RIB.

Si ces documents lui sont effectivement transmis, il pourra par la suite usurper l’identité de sa victime.

L’usurpateur peut « simplement » vouloir **nuire à votre réputation** :

Une fois en possession de vos données personnelles (comme vos nom, prénom, âge, coordonnées et photo), il sera alors en mesure de créer un compte sur un réseau social, ou encore un faux profil sur un forum de discussion, ou même un blog, en votre nom.

Il pourra ensuite s’exprimer comme bon lui semble : s’il lui prenait l’envie d’écrire des commentaires racistes ou des articles haineux, les internautes penseront malheureusement que vous en êtes l’auteur, puisqu’il agit en empruntant votre identité.

Ou l'usurpation peut avoir un caractère plus « dangereux » :

Reprenons l’exemple cité au début de ce chapitre et supposons qu’un internaute, à la recherche d’un appartement à louer, ait envoyé les documents demandés par l’usurpateur.

Ce dernier a à présent toute liberté d'utiliser les documents pour souscrire des crédits, tels les crédits à la consommation pour lesquels aucun autre document ne sera exigé.

Une fois l'argent à sa disposition, l'escroc en profitera librement, tandis que l'organisme prêteur se tournera vers la victime pour obtenir le remboursement de la somme empruntée.

Protégez-vous de l'usurpation d'identité

Les informations utilisées à des fins d'usurpation d'identité sont généralement obtenues de manière frauduleuse. Les usurpateurs ont malheureusement plusieurs moyens à leur disposition. Les renseignements peuvent notamment être obtenus :

- via une opération de phishing ;
- grâce à un vol de mots de passe ;
- ou être le résultat d'une escroquerie (via la publication de petites annonces pour un appartement à louer, par exemple).

Pour vous protéger, suivez les conseils prodigués dans les précédents chapitres de ce cours :

- soyez prudent lorsque vous communiquez des données personnelles sur Internet ;
- vérifiez la fiabilité des sites sur lesquels vous êtes amené à saisir des informations ;
- soyez attentif aux courriels arrivant dans votre boîte de réception, afin de reconnaître d'éventuelles tentatives d'hameçonnage ;
- effacez régulièrement les cookies et les données de navigation de votre navigateur Internet ;
- choisissez des mots de passe forts et efficaces.

Que faire si vous êtes victime d'une usurpation d'identité ?

Si vous vous apercevez que votre identité a été usurpée, la première chose à faire est de collecter le plus d'éléments possibles afin de pouvoir **apporter les preuves** de cette infraction.

Bien que cela puisse paraître quelque peu injuste, **la loi indique en effet qu'il incombe à la victime de fournir la preuve que son identité a été usurpée**.

À cette fin, il vous faudra récolter un maximum d'informations : il s'agit le plus souvent des captures d'écran sur lesquels apparaissent votre photo et/ou vos

données personnelles, des adresses des pages Internet concernées, et de tout autre justificatif ou document qui vous semblera pertinent.

Une fois que vous aurez rassemblé ces différents éléments, il vous faudra **prévenir les responsables des sites** sur lesquels s'est produite l'usurpation et leur demander de supprimer le plus rapidement possible toutes les données vous concernant.

> Si l'usurpateur a créé un compte en votre nom (un faux profil Facebook, par exemple), il faudra également exiger la fermeture de ce compte ou profil.

La grande majorité des sites disposent d'un **service de réclamation** accessible en ligne ; si ce n'est pas le cas, vous pourrez vous adresser à leur service client qui soit traitera votre demande, soit vous orientera vers le bon interlocuteur.

Avant de traiter votre demande, le site concerné vous demandera de prouver votre identité.
Ce qui peut être fait tout simplement en lui transmettant une copie recto-verso de votre pièce d'identité, et en y ajoutant, selon les cas, une photo de vous (récente).

Dans le cas précis où un usurpateur a souscrit un ou plusieurs crédits en votre nom et que les organismes concernés vous demandent le remboursement de ces crédits, il est conseillé de les joindre aussitôt par téléphone afin d'expliquer votre situation et connaître l'ensemble des documents à fournir pour prouver vos dires.

Vous devrez ensuite envoyer une **lettre recommandée** indiquant les circonstances de l'usurpation, en y joignant l'ensemble des preuves que vous aurez récoltées, ainsi que la copie de votre pièce d'identité accompagnée d'une attestation sur l'honneur manuscrite disant que vous n'avez jamais souscrit ce(s) crédit(s).

S'il faut bien entendu alerter les sites Internet concernés afin de mettre fin à l'usurpation ; cela n'aura toutefois aucun impact sur l'usurpateur lui-même.

> L'usurpation d'identité constitue pourtant un délit puni par la loi française d'une peine d'emprisonnement pouvant aller jusqu'à un an d'incarcération, et/ou d'une amende d'un montant maximum de 15 000 €.

Si vous souhaitez que l'auteur de l'infraction soit sanctionné, vous pouvez **porter plainte**, soit au commissariat de police, soit à la gendarmerie de votre domicile. Il est également possible de commencer la démarche en ligne : en déposant une préplainte sur le site https://www.pre-plainte-en-ligne.gouv.fr/. Vous serez tout de même obligé de vous déplacer par la suite, afin de signer votre déclaration dans une unité de gendarmerie ou un commissariat.

Si l'usurpateur est identifié (malheureusement, c'est rarement le cas) et poursuivi par la justice, la victime peut demander le **versement de dommages et intérêts**.

Certaines assurances habitation proposent d'ailleurs de nos jours des options « *Usurpation d'identité* » ; un bon moyen d'être indemnisé en cas de délit à votre encontre.

Minimisez les risques d'atteinte à votre vie privée

L'usurpation d'identité n'est pas le seul risque auquel nous pouvons être exposés en naviguant sur Internet. Nous avons en effet pu voir au cours des précédents chapitres que notre activité sur la toile est surveillée et enregistrée par différentes sociétés.

Pour restreindre les données auxquelles elles peuvent avoir accès et ainsi mieux protéger votre vie privée, voici quelques conseils à suivre.

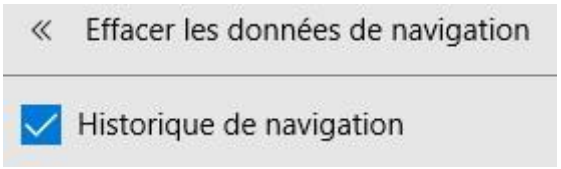
Supprimez l'historique de votre navigateur

Votre historique, qu'il s'agisse de navigation ou de recherches, contient les adresses de tous les sites et de toutes les pages que vous avez visités (historique de navigation) ainsi que l'ensemble des recherches que vous avez effectuées sur Internet (historique du moteur de recherche).

Il est donc susceptible de refléter vos goûts, préoccupations et centre d'intérêts, toutes choses qui relèvent de la sphère privée et qu'il convient de protéger.

Microsoft Edge

1. Cliquez sur le bouton **Paramètres**  en haut à droite de l'écran puis sur ***Paramètres***.
2. Dans la rubrique ***Effacer les données de navigation***, cliquez sur ***Choisir les éléments à effacer***.
3. Cochez la case **Historique de navigation** puis cliquez sur ***Effacer***.



Firefox

1. Cliquez sur le bouton **Options**  puis sur ***Options***.
2. Cliquez sur ***Votre** bibliothèque.* 
3. Cliquez sur le panneau **Historique** puis sur ***Supprimer l'historique récent***.
4. Choisissez la période de temps que vous voulez supprimer.
5. Cliquez sur ***Effacer maintenant***.

Chrome

1. Cliquez sur le bouton **Options** ⋮ en haut à droite de l'écran puis sur ***Paramètres***.
2. À gauche, cliquez sur ***Paramètres avancés*** puis sur ***Confidentialité & sécurité***.
3. Cliquez sur ***Effacer les données de navigation*** et cochez la case ***Historique de navigation***.
4. Choisissez la période souhaitée puis cliquez sur le bouton ***Effacer les données***.

Safari

1. Cliquez dans la barre de menus sur ***Historique*** puis sur ***Effacer l'historique***.
2. Cliquez sur le **menu local** & indiquez la **période** pour laquelle vous voulez effacer l'historique.

Supprimez l'historique de vos moteurs de recherche

À la différence de votre historique de navigation, l'historique de vos recherches n'est pas enregistré sur votre ordinateur, mais sur les serveurs du moteur de recherche. Cet historique est associé à votre compte sur le moteur de recherche utilisé.

Sans intervention de votre part, il est généralement conservé très longtemps (plusieurs années).

Google

1. Connectez-vous à votre compte Google.
2. À gauche, cliquez sur ***Données et personnalisation***.
3. Cliquez sur ***MonActivité***.
4. Dans le volet gauche, cliquez sur ***Supprimer l'activité***.
5. Sélectionnez la période souhaitée.
6. Sélectionnez ***Supprimer***.

Bing

1. Accédez à **Bing** sur le navigateur de votre choix.

2. Cliquez sur **l'icône *Paramètres*** (représentée par un engrenage) en haut à droite de la page.
3. Cliquez sur ***Historique de recherche***.
4. Cliquez sur la **flèche vers le bas** près de "***Changer les préférences de l'historique***".
5. Sous "***Changer les préférences de l'historique***", cliquez sur le bouton ***Tout effacer***.

Supprimez votre activité sur Facebook

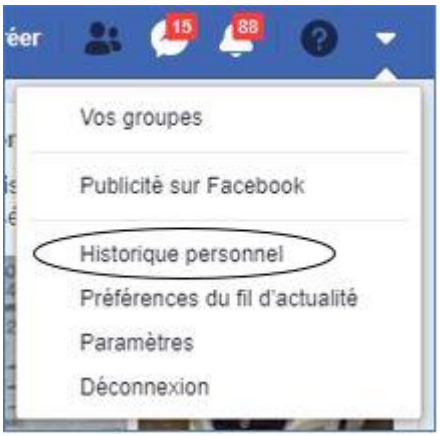
> Votre historique sur Facebook contient toutes vos publications, activités et actions, ainsi que les articles vous mentionnant et les photos sur lesquelles vous apparaissez. Il comprend également la listes des recherches que vous avez effectuées sur Facebook. Par défaut, cet historique n'est jamais supprimé.

Bien qu'il ne soit accessible qu'à vous seul, chacun des éléments archivés apparaît forcément ailleurs sur Facebook (par exemple dans votre journal, ou dans le fil d'actualité de vos amis).

Certaines actions ou publications peuvent ainsi dater de plusieurs mois ou plusieurs années, et ne plus refléter votre pensée actuelle.

Pour protéger votre intimité, voici comment effacer cet historique :

Cliquez sur le bouton  en haut à droite de n'importe quelle page Facebook,



Puis, cliquez sur Historique personnel

Le volet **Filtres** à gauche de l'écran permet de choisir la catégorie d'archives que vous souhaitez consulter.

Volet Filtres de votre compte Facebook

Et dans la partie droite, vous trouverez une échelle permettant d'afficher les données par année (de la première année d'utilisation de Facebook à aujourd'hui.)

L'échelle de temps à droite de votre écran

Facebook n'offre aucune possibilité de supprimer l'intégralité de l'historique en un clic.

Commencez par choisir la catégorie d'éléments à afficher en utilisant le volet des filtres puis cliquez sur l'année souhaitée.

Vous devrez ensuite supprimer les éléments un par un en cliquant sur le bouton ***Modifier*** (représenté par un **petit crayon**) puis sur ***Supprimer***.

Bouton pour modifier

Pour accéder à l'**historique de vos recherches sur Facebook**, il vous faudra en outre cliquer sur la mention ***Plus*** dans le bas du volet gauche puis sur ***Historique de Recherches***.

> Là encore, vous ne pourrez supprimer toutes les recherches en un clic. Il faudra de nouveau les effacer une à une.

Cliquez sur le bouton "plus"

> Seule la catégorie **Photos** vous permettra d'en sélectionner plusieurs, ou même de les sélectionner toutes pour les supprimer en une seule fois.

Effacez l'historique des vidéos regardées

Lorsque vous utilisez un service comme **YouTube**, l'historique des vidéos que vous visionnez est activé par défaut et sera conservé tant que vous ne le supprimerez pas.

Cette option facilite vos recherches en permettant de mémoriser les dernières vidéos regardées et d'obtenir des propositions censées vous correspondre dans la rubrique ***Recommandations***.

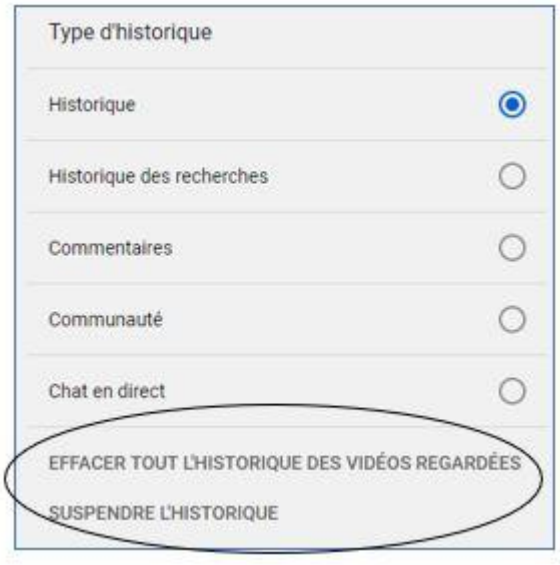
> **YouTube** offre la possibilité de supprimer, totalement ou partiellement, l'historique, et également de le désactiver.

Comme tous les historiques cités précédemment, il n'est normalement accessible qu'à vous et à vous seul. Cependant, si vous utilisez un ordinateur partagé avec des membres de votre famille (par exemple), ou en cas de piratage, vous ne pouvez être

absolument certain que cet historique ne sera jamais vu par un autre que vous. À moins que vous ne l'effaciez régulièrement :

- rendez-vous sur le site YouTube (https://www.youtube.com/) ;
- dans le volet de gauche, cliquez sur ***Historique***.

Dans le volet de droite, cliquez sur ***Effacer tout l'historique des vidéos regardées*** et, si vous souhaitez désactiver cette option à l'avenir, cliquez ensuite sur ***Suspendre l'historique***.



Menu d'accès sur YouTube

Effacez l'historique des conversations privées

La suppression de votre activité sur Facebook, dont nous avons parlé dans le précédent paragraphe, ne permet toutefois pas d'effacer l'historique de vos conversations privées. Pour ce faire :

1. Cliquez sur le bouton **Messenger** en haut de la page.
2. Cliquez sur la conversation à supprimer.
3. Cliquez sur le bouton **Options** en haut de la fenêtre, puis sur ***Supprimer la conversation***.

Pour effacer l'intégralité de l'historique, vous devrez de nouveau supprimez **une à une** chaque conversation.

> Sachez cependant que les messages que vous avez écrits et lus demeurent présents dans la boîte de réception de votre interlocuteur. Le fait de les effacer de votre compte n'entraîne pas leur suppression dans les comptes de vos amis.

Le RGPD

Le **RGPD** (**R**ègle**G**énéral sur la **P**rotection des **D**onnées) ou en anglais GDPR (*General Data Protection Regulation*) est entré en vigueur le 25 mai 2018.
L'objectif premier de ce règlement européen était de permettre d'harmoniser les différentes lois sur la protection des données existant dans chaque pays membre.
Le RGPD ayant dorénavant fonction de loi officielle sur la protection des données pour tous les états membres, il prévaut sur les lois nationales en vigueur.

Il permet de **mieux protéger** les données personnelles des particuliers et des salariés, et impose **plus de contraintes aux organismes collecteurs** : les entreprises employant des salariés sont tenues de respecter le RGPD et en cela de garantir la protection de la vie privée des employés, ainsi que celle des données récoltées sur leurs clients & fournisseurs.

Toute entreprise qui récolte des données doit ainsi **informer clairement** les internautes de la collecte et du type de données récoltées, et préciser son objectif qui devra être obligatoirement respecté. L'entreprise devient responsable des données récoltées. Elle a le devoir d'assurer leur protection : ce qui lui interdit donc de les communiquer à d'autres organismes sans l'accord préalable des individus concernés, et lui impose de sécuriser les données afin qu'elles ne puissent être piratées.

Par exemple, une société qui rassemble des données dans le but de signer un contrat n'aura pas le droit d'utiliser ces mêmes données à des fins publicitaires.

Enfin, les sociétés sont également tenues de collecter le moins de données possibles (uniquement celles qui sont absolument nécessaires à la réalisation de l'objectif précédemment annoncé) et leur durée de conservation est limitée (une fois le but atteint, les données doivent être supprimées).

Le RGPD conforte également un droit fondamental en réaffirmant que **chacun est maître de ses données personnelles**, avec le pouvoir de décider de leur traitement : en clair, il est interdit de publier sur Internet ou d'utiliser (à des fins publicitaires, par exemple) les données personnelles d'un individu sans l'accord de ce dernier.

Chacun d'entre nous peut demander à contrôler les données personnelles détenues par une entreprise et exiger leur modification ou leur suppression.

Le RGPD impose en outre aux organismes collecteurs le respect du **droit à la portabilité** :

Supposons que vous ayez souscrit un abonnement Internet chez Free ; un an plus tard, vous souhaitez changer de fournisseur d'accès : grâce au droit à la

portabilité, Free est obligé de transmettre toutes les données vous concernant à votre nouveau fournisseur.

Enfin, le RGPD stipule qu'il est obligatoire d'informer les particuliers en cas de piratage des données.

Accédez à vos données personnelles

Vous avez donc le droit de demander à une entreprise ou un organisme s'il détient des données personnelles vous concernant et si oui, dans quel but. Votre interlocuteur a obligation de vous répondre.

Supposons que vous soyez client d'un site de vente en ligne sur lequel vous passez régulièrement des commandes. Vous demandez à l'entreprise de consulter vos données personnelles.

Le site vous transmet alors une copie de ces données dans un document qui contiendra les informations suivantes : vos nom, prénom, adresse postale, adresse mail, téléphone, nombre de commandes passées sur le site, dates des commandes, liste des articles achetés, nombre de retours effectués, ainsi que, le cas échéant, les publicités dont vous auriez été la cible et les noms des entreprises partenaires auxquelles ont été transmises vos données.

Imaginons maintenant que vous êtes également inscrit sur un réseau social auquel vous demandez une copie des données vous concernant. Les informations qu'il est tenu de vous faire parvenir seront cette fois composées de : vos nom, prénom, adresse postale, adresse mail, téléphone, photo, mais aussi de tous les messages et commentaires que vous avez écrits ou reçus, des photos que d'autres vous ont envoyées et de la liste de toutes les actions que vous avez effectuées sur le site depuis votre inscription.

Rectifiez ou supprimez vos données personnelles

En plus du droit de consultation de vos données à caractère personnel, vous avez le **droit** de demander à une entreprise de **supprimer** vos données personnelles, notamment lorsque ces données sont utilisées à des fins publicitaires.

Attention toutefois, ce droit a lui-même des limites : il peut en effet s'exercer tant qu'il ne porte pas atteinte aux droits et libertés d'autrui. Ainsi, il pourra être abrogé dans les cas suivants :

- le traitement des données sert l'intérêt public (pour des recherches scientifiques ou historiques par exemple, ou encore l'établissement de statistiques) ;

- les données détenues participent à l'exercice du droit à la liberté d'expression ou à celui de la propriété intellectuelle ;
- une obligation légale impose de les conserver.

Prenons un premier exemple :

> Imaginez une personne férue d'escalade en montagne, qui pratique régulièrement dans la région de Chamonix et que nous appellerons madame Dupont. L'office du tourisme de la ville lui demande si elle serait d'accord pour écrire un article sur le sujet, afin qu'il soit publié sur leur site Internet.
>
> Mme Dupont écrit un fort bel article, qui vante à la fois les mérites de l'escalade et ceux de la région. L'article est publié sur le site, indiquant comme il se doit les nom, prénom et activité de l'auteur.
>
> Un an plus tard, madame Dupont, pour des raisons d'ordre privé, demande à l'office du tourisme la suppression de toutes les données personnelles la concernant. Sa demande devra être étudiée, mais il n'est pas certain que l'office du tourisme y accède : elle peut en effet empiéter sur la liberté d'autrui et se heurter à la notion de propriété intellectuelle.

En voici un second :

> Un journaliste publie un article sur le site d'un journal ayant pour sujet une actrice célèbre et décrivant les excès auxquelles celle-ci s'est livrée pendant ses vacances à Ibiza. L'actrice concernée demande la suppression de toutes les données la concernant.
>
> Là encore, le site n'est pas tenu d'accéder à sa demande ; il peut en effet arguer que cette dernière empiète sur les principes fondamentaux de la liberté d'expression.

Dans la plupart des cas toutefois, la demande de suppression apparaît totalement légitime et l'organisme concerné n'a d'autre choix que d'y accéder.

L'exemple le plus courant étant celui du client qui ne veut plus être noyé sous les publicités.

> J'ai ainsi connu un jeune homme qui, après avoir acheté en ligne des billets pour un festival de musique un été, ne cessait de recevoir des publicités pour des spectacles et des concerts.
>
> Il a contacté le site qui lui avait vendu les billets afin d'exercer son droit de rectification : sans exiger la suppression de ses données personnelles, il a en

effet demandé une modification de leur traitement. À savoir, qu'elles ne soient plus ni utilisées ni transmises à des tiers à des fins publicitaires. Sa demande a été entendue et les publicités ont cessé d'affluer.

Et en voici un dernier exemple, ayant tendance à se multiplier :

Le cas de personnes qui, ayant publié des photos, messages et/ou commentaires sur des réseaux sociaux durant leur adolescence, craignent une fois adultes que ces éléments n'aient des conséquences négatives sur leur vie professionnelle, et demandent la suppression de ces données.

Si ces personnes étaient mineures au moment où elles étaient actives sur le réseau, ce dernier a l'obligation de satisfaire leur demande et donc de supprimer tout contenu les concernant, et également celle d'informer les autres sites partenaires de la volonté de suppression ainsi exprimée.

En résumé

- L'usurpation d'identité consiste à utiliser vos données personnelles sans vous avoir demandé votre accord au préalable, dans le but de nuire à votre réputation ou de mener en votre nom des opérations visant à dérober de l'argent.
- Pour vous protéger, ne communiquez vos données personnelles qu'avec parcimonie, contrôlez la fiabilité des sites que vous visitez, soyez attentif aux courriels reçus afin d'éviter les tentatives de phishing, maîtrisez les traces de votre navigation et choisissez de bons mots de passe.
- Si vous êtes malgré tout victime d'usurpation de votre identité, récoltez le maximum de preuves avant de prévenir le site concerné.
- Pour mieux protéger votre vie privée, pensez à supprimer régulièrement vos différents historiques : historique de navigation, du moteur de recherches, de votre activité sur Facebook, des conversations privées et des vidéos regardées.
- Le RGPD garantit la protection de vos données personnelles et définit les obligations des organismes collecteurs. Il vous donne notamment la possibilité de contrôler, rectifier et supprimer les données personnelles qui vous concernent.

Soignez votre e-réputation

Distinguez clairement sphère privée et publique

Faites attention aux photos et aux vidéos

Les internautes de tous âges sont de plus en plus nombreux à publier leurs photos sur Internet, sur des sites de réseaux sociaux dans la majorité des cas.

> Ainsi, selon une étude TNS Sofres, plus de 50 % des internautes (tous âges confondus) disent partager leurs photos (via un blog, une page Facebook ou un site Internet), tandis que ce chiffre atteint 86 % chez les 18-24 ans.

Publier des photos de famille, de vacances, ou encore de soirées entre amis, paraît de prime abord tout à fait innocent et plutôt sympathique ; et ce serait effectivement le cas si le monde n'était peuplé que de personnes bien intentionnées.

Mais dans la réalité, la publication de photos en ligne n'est pas sans risque…

> On peut prendre pour exemple ces adolescents qui publient des photos de soirées un peu trop arrosées sur Facebook, et qui bien souvent le regrettent quelques années plus tard.
> La publication de certaines photos peut ainsi donner une fausse image de vous et entacher votre réputation.

Les enfants sont également concernés : de plus en plus de parents partagent très régulièrement les photos de leurs bébés et enfants sur Internet. Ce qui pose un premier problème : celui du respect de l'intimité de ces enfants.

> Imaginez que vous découvrez des photos de vous sur la toile, prises à l'âge de 18 mois, quand vous étiez assis sur le pot ou nu dans votre bain : vous seriez parfaitement en droit de ne pas apprécier ! 

Certains enfants sont d'ailleurs moqués par leurs camarades d'école à cause des photos publiées par leurs parents sur le web. Tout cela est encore plus vrai lorsqu'il s'agit de vidéos : une photo fixe un instant précis, mais une vidéo expose davantage notre intimité.

> Dès lors qu'il s'agit d'enfants, le risque est autrement plus sérieux : les photos peuvent en effet être récupérées par des personnes mal intentionnées et détournées de leur usage premier.

En 2016, la gendarmerie française a ainsi publié un message sur son compte Facebook pour inciter les familles à une plus grande prudence : elle avait eu connaissance de photos d'enfants dérobées sur des sites et réseaux sociaux et publiées par la suite sur des sites de pédopornographie.

Il faut donc avoir conscience qu'une photo partagée en ligne n'est plus totalement sous votre contrôle. Même si vous décidez par la suite de la supprimer, il est toujours possible que quelqu'un en ait fait une capture d'écran pour la publier sur un autre site, ou simplement pour la conserver sur son disque dur.

Pour mieux vous protéger, vous trouverez ci-dessous quelques règles de prudence préconisées par la **Cnil** (**C**ommission **N**ationale **I**nformatique & **L**iberté) :

1. Prenez toujours le temps de **bien réfléchir avant de publier** une photo, en ayant à l'esprit qu'il peut être difficile, et parfois impossible (si la photo a été copiée ou partagée), de la supprimer plus tard.
2. Ne publiez pas de photos de quelqu'un sans avoir obtenu son **autorisation au préalable**.
3. Modifiez les **paramètres de confidentialité** de votre compte Facebook, de manière à bien définir les autorisations d'accès à vos photos.
4. **Adaptez les publications** de vos photos selon les sites : sur Instagram, par exemple, il est impossible de restreindre l'accès aux photos : elles sont accessibles à tout le monde. Il vaut donc mieux soit éviter de publier des photos sur ce type de site, soit n'y publier que celles qui révèlent le moins votre vie privée.
5. Utilisez avec modération les **outils d'identification** (tags) et de reconnaissance faciale qui exposent davantage les personnes.
6. Consultez régulièrement vos photos et, le cas échéant, n'hésitez pas à demander la suppression de celles qui pourraient devenir gênantes.

Soyez prudent sur les réseaux sociaux

Les conseils que nous avons évoqués au sujet de la publication de photos et vidéos demeurent valables pour toute activité que vous êtes susceptible d'avoir sur les réseaux : réfléchissez bien avant de publier des messages ou des commentaires.

- Peuvent-ils blesser ou déranger quelqu'un ?
- Sont-ils susceptibles de vous embarrasser ou de vous gêner dans le futur ?

Si vous répondez oui à l'une de ces questions, mieux vaut vous abstenir.

Sur des sites de réseaux sociaux, il peut arriver qu'une personne qui vous est totalement inconnue demande à être votre amie : il **vaut mieux dans ce cas ne pas accepter**.

N’oubliez pas que vos amis sur Facebook ont **accès à de nombreuses informations** personnelles vous concernant.

Restez dans tous les cas très prudent lorsque vous échangez avec des inconnus.

Paramétrer vos comptes pour limiter votre visibilité

Tout ce que vous publiez sur les réseaux sociaux est, par défaut, visible publiquement.

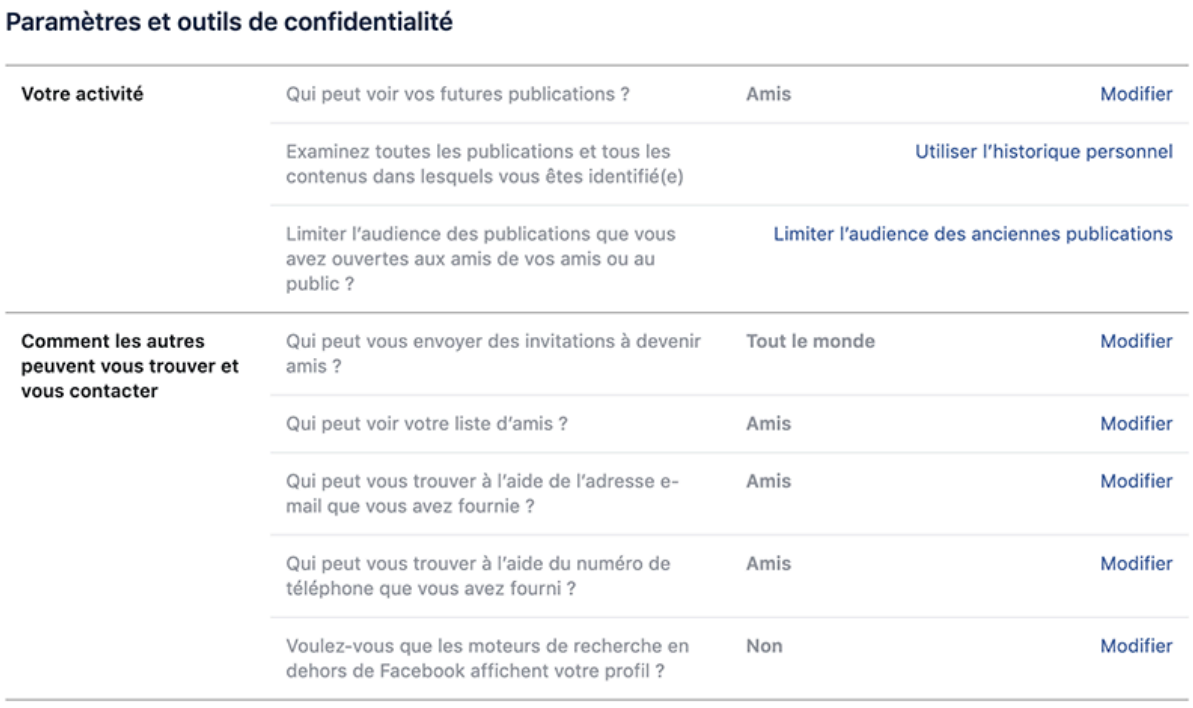
Pour que votre compte et vos publications ne soient accessibles qu’à vos amis et entourage, suivez la procédure ci-dessous :

1. Rendez-vous sur votre page **Facebook**.

2. Cliquez sur ▼ (en haut à droite).

3. Cliquez sur ***Paramètres***.

4. À gauche, cliquez sur ***Confidentialité***.

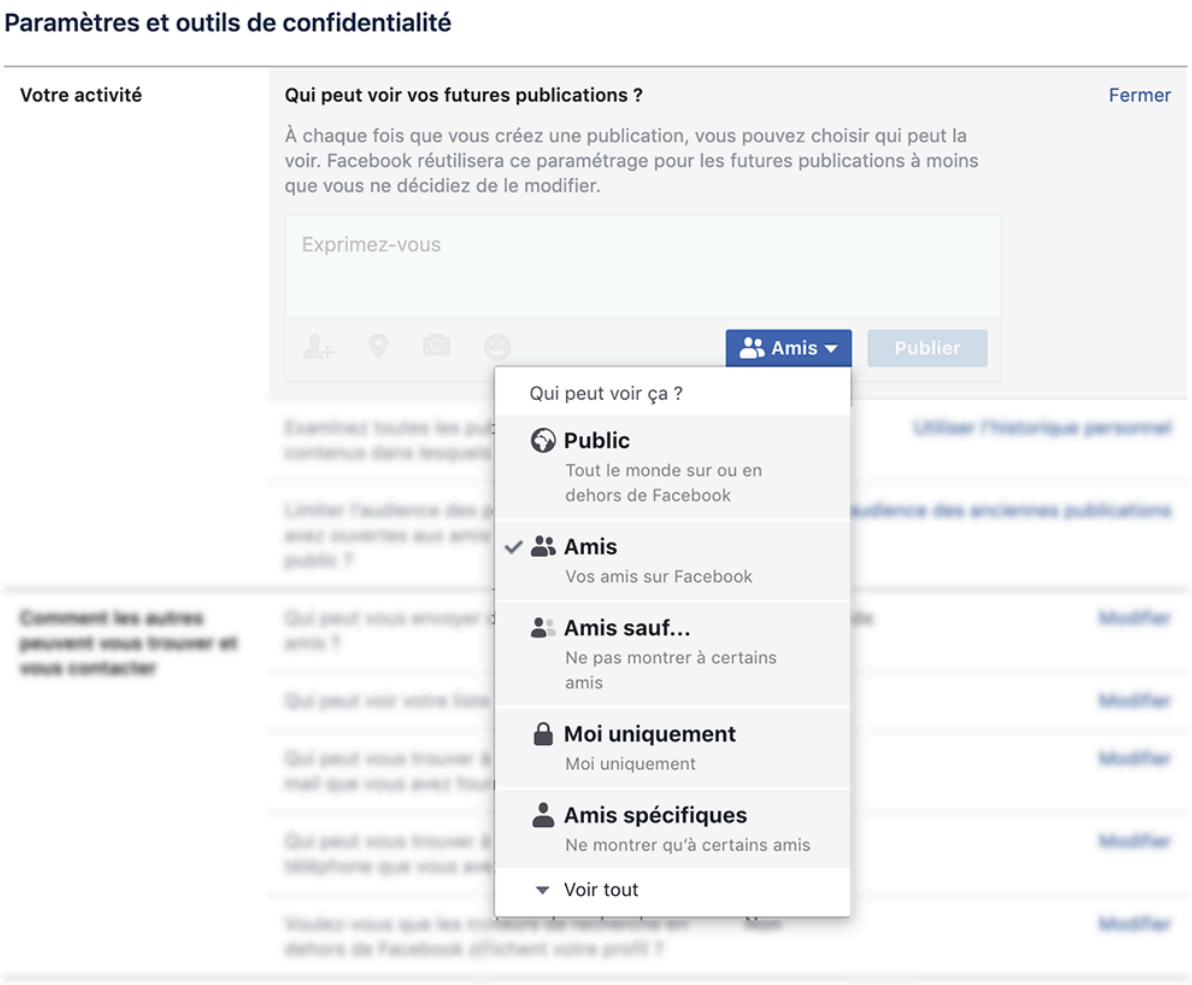


Paramètres et outils de confidentialité

Votre activité	Qui peut voir vos futures publications ?	Amis	Modifier
	Examinez toutes les publications et tous les contenus dans lesquels vous êtes identifié(e)		Utiliser l’historique personnel
	Limiter l’audience des publications que vous avez ouvertes aux amis de vos amis ou au public ?		Limiter l’audience des anciennes publications
Comment les autres peuvent vous trouver et vous contacter	Qui peut vous envoyer des invitations à devenir amis ?	Tout le monde	Modifier
	Qui peut voir votre liste d’amis ?	Amis	Modifier
	Qui peut vous trouver à l’aide de l’adresse e-mail que vous avez fournie ?	Amis	Modifier
	Qui peut vous trouver à l’aide du numéro de téléphone que vous avez fourni ?	Amis	Modifier
	Voulez-vous que les moteurs de recherche en dehors de Facebook affichent votre profil ?	Non	Modifier

Les paramètres de confidentialité sur Facebook

5. Dans la partie, « Activités », rubrique « *Qui peut voir vos futures publications ?* », cliquez sur **Modifier :**



Choisissez une option parmi les choix proposés

L'option « amis spécifiques » réserve l'accès à vos publications à certains de vos amis seulement tandis que « amis sauf… » permet à l'inverse d'exclure certaines personnes de votre choix.

6. Cliquez ensuite sur ***Fermer***, en haut à droite de cette rubrique.

7. Cliquez sur ***Limiter l'audience des anciennes publications*** pour que ces dernières ne soient accessibles qu'à vos amis (et cela même si elles étaient publiques auparavant)

8. La rubrique « ***Comment les autres peuvent vous trouver et vous contacter*** » vous permet de renforcer davantage encore vos paramètres de confidentialité, en restreignant par exemple le nombre de personnes habilitées à vous envoyer une invitation ou en limitant la consultation de votre liste d'amis.

S'il est prudent de réserver la lecture de vos publications à vos seuls amis, cette manipulation est **sans effet sur vos photos**.

Mais, heureusement, il est possible ici aussi de restreindre l'accès des photos. Pour cela :

1. Rendez-vous sur votre page Facebook et cliquez sur ***votre nom*** (en haut à gauche).
2. Cliquez sur ***Photos***, puis sur ***Albums***.
3. Cliquez sur l'album dont vous voulez modifier les paramètres de confidentialité.
4. Cliquez sur ***Modifier*** en haut à droite.
5. Cliquez sur ***Confidentialité*** pour contrôler qui peut voir votre album.

Seule la personne ayant publié l'album peut modifier ses paramètres de confidentialité.

Surveillez les publications vous concernant

Vérifiez régulièrement ce qui est publié

Pour conserver une bonne e-réputation, une attitude prudente et réfléchie sur les réseaux sociaux est essentielle, mais cela n'est **pas toujours suffisant**. D'autres que vous peuvent en effet publier et partager sur Internet des informations vous concernant, ou des photos sur lesquelles vous apparaissez.

Il existe un moyen à la portée de tous de vérifier rapidement si des publications vous impliquant ont paru sur le web : **tapez vos nom & prénom sur Google** ou tout autre moteur de recherches.

- Si **aucun résultat** ne s'affiche, c'est que vous n'êtes **pas présent sur la toile** : votre réputation ne risque donc absolument rien.
- Si, au contraire, vous obtenez des résultats, il convient alors de les **consulter un à un**.
  Pour chacun, commencez par vérifier qu'il **s'agit bien de vous** ! Nous avons en effet tous plus d'homonymes que nous ne le pensons.
- Si certains résultats vous concernent personnellement et qu'ils vous semblent **préjudiciables** à votre réputation, **notez les adresses des sites** concernés (au besoin, vous pouvez également réaliser des captures d'écran) puis reportez-vous à la suite de ce cours pour savoir comment demander la **suppression de ces données**.
- Pensez également à cliquer sur les onglets ***Images*** et ***Vidéos*** dans la page de résultats de vos recherches. Vous pouvez en effet être absent des publications écrites tout en étant identifié sur une photo ou vidéo partagée en ligne par l'un de vos amis.

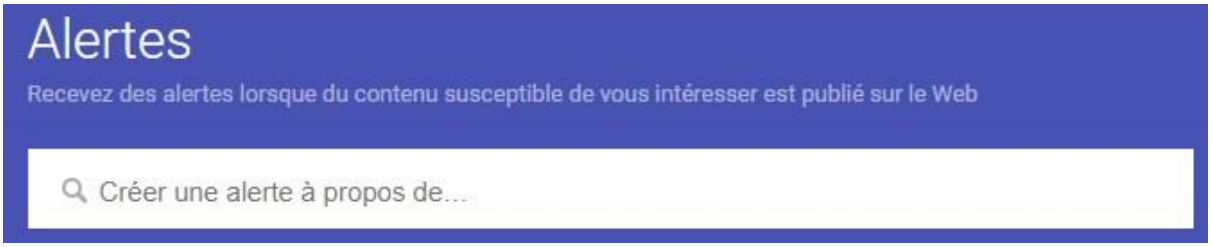
La notion de e-réputation est un phénomène récent, apparu conjointement au développement d'Internet, et plus particulièrement des réseaux sociaux.

Un nombre croissant d'internautes est ainsi soucieux de cette réputation « par écrans interposés » ; pour leur permettre de surveiller les publications pouvant apparaître sur leur compte, des entreprises ont créé des outils de surveillance de la toile. Leur fonction est de vous alerter dès qu'un nouvel élément (texte, photo ou vidéo) vous concernant s'affiche sur Internet.

Les outils d'alerte

Parmi ces outils, il en existe notamment 3 dont l'usage est simple et gratuit :

- Google Alertes



Pour être averti lorsque quelqu'un publie un élément vous concernant : il suffit d'indiquer vos nom & prénom, puis de cliquer sur le bouton ***Créer une alerte***.

En cliquant sur le bouton ***Modifier*** (représenté par un petit crayon), vous pourrez ensuite choisir par exemple la fréquence de réception des alertes (qui vous seront transmises par mail), leurs sources (sites Internet, blogs, vidéos, actualités, etc.), ou bien conserver les paramètres existants par défaut.

Pour éviter de recevoir trop de mails liés aux alertes, vous pouvez demander à les recevoir toutes rassemblées dans un mail unique. Pour cela, cliquez sur le bouton

Options (représenté par une petite roue crantée) et cochez la case ***Récapitulatif***.

- Mention
- Alerti

Comme Google Alertes, ces deux outils permettent de surveiller toute donnée pouvant paraître sur vous sur la toile, incluant les réseaux sociaux, sites d'actualités, blogs, images, vidéos et forums.

À vous de choisir celui des 3 qui vous conviendra le mieux !

Pouvoir surveiller sa e-réputation, c'est très bien… mais agir pour supprimer tout ce qui pourrait lui nuire est encore mieux ! Étudions cela.

Réclamer la suppression des contenus portant atteinte à votre vie privée

> Selon la loi, vous avez le droit de demander la suppression de données vous concernant, à condition que celles-ci aient un caractère erroné, obsolète ou encore préjudiciable.

Vous devez pour cela envoyer une demande au responsable du site sur lequel elles ont été publiées. Il reste cependant à trouver ses coordonnées ! La plupart du temps, elles sont indiquées dans les mentions légales ou bien dans les CGU (conditions générales d'utilisation) du site. Si jamais elles n'y figuraient pas, vous pouvez tenter de les retrouver en consultant le Whois : le nom du responsable du site y est normalement inscrit à la rubrique « *propriétaire du nom de domaine* ».

Le responsable du site Internet concerné devra examiner votre demande et vous apporter une réponse dans un **délai de 2 mois maximum**. Pour avoir des chances d'être acceptée, celle-ci devra être **justifiée** : il vous faudra expliquer en quoi ces informations peuvent nuire à votre réputation ou à votre vie privée.

> Afin d'aider les internautes dans leurs démarches, la CNIL publie un **modèle de courrier** à reproduire, que je vous invite à réutiliser si besoin.

Si malgré votre demande, le site manquait à son obligation de réponse, vous pourrez adresser une plainte à la CNIL, via un formulaire en ligne. Sachez que si vous recevez une réponse négative, il vous reste un moyen d'action : demander le **déréférencement de vos données**.

Le déréférencement d'un contenu vous concernant

Le déréférencement de pages Internet signifie que ces pages ne seront plus indexées par les moteurs de recherche. C'est-à-dire qu'elles seront absentes des résultats des recherches effectuées. Ainsi, demander le déréférencement de contenus vous concernant consiste donc à demander la suppression de certains résultats de recherche liés à vos nom & prénom.

Pour autant, ces pages existeront toujours et **demeureront accessibles** aux internautes sur les sites qui les ont publiées. Elles restent donc sur le web, mais deviennent simplement difficiles à trouver.

Pour bien comprendre, prenons l'exemple d'Albert Martin :

Imaginez qu'en tapant son nom et son prénom sur Google, on obtienne une page de résultats dont le premier renvoie vers les photos d'une soirée un peu trop arrosée… Albert y apparaît en effet une bouteille à la main, vêtu en tout et pour tout d'une coiffe d'Indien !
Or, il a l'intention de postuler prochainement pour un nouveau travail. Il sait que les recruteurs ont l'habitude faire des recherches en ligne sur les candidats, et il craint que ce résultat ne joue pas en sa faveur…

Heureusement, il existe un recours légal : la Cour de justice de l'Union européenne a, en mai 2014, réaffirmé la notion de **droit à l'oubli numérique**, suivant lequel tout citoyen européen a le droit de demander l'effacement de résultats de recherches le concernant.

Depuis le mois de mai 2014, les moteurs de recherche ont donc obligation de mettre à la disposition de leurs utilisateurs un « ***formulaire de droit à l'oubli*** » ou « *formulaire de demande de suppression* ».

Ils doivent ensuite examiner les demandes qui leur sont adressées et transmettre leur **réponse dans un délai d'un mois** (pouvant être allongé à 3 mois si la demande est complexe).

Si la demande porte sur des **mineurs**, le déréférencement sera **forcément accepté**. Et c'est le cas également pour toute demande concernant des **informations erronées** ou falsifiées, des informations **diffamatoires**, injurieuses, ou si elles reflètent une opinion plutôt que des faits.

Déférencez des informations

Pour demander le déférencement d'informations vous concernant, il vous faut accéder au formulaire de demande de suppression. Pour cela, cliquez sur les liens suivants :

- Google (Cochez ensuite l'option : *Je voudrais supprimer mes informations personnelles des résultats de recherche Google.*)
- Bing
- Yahoo

Il est conseillé de garder une preuve de votre démarche (par exemple une capture d'écran).
Cela peut en effet être utile si votre demande était refusée et que vous souhaitiez en référer à la CNIL.

Ce que dit la loi

Le rôle de la CNIL

Créée au mois de janvier 1978, la **CNIL** est un organisme public responsable de la protection des données personnelles.

La CNIL s'appuie sur un principe simple : l'informatique doit être au service des citoyens et ne doit pas porter atteinte aux droits des individus, non plus qu'à leur vie privée ou à leur liberté.

Son rôle est d'informer le public de ses droits, de conseiller les entreprises et les individus, d'alerter en cas de non-respect des lois, mais aussi de contrôler et de sanctionner les responsables d'éventuels écarts.

En cela, elle doit aider les entreprises et les organismes qui traitent des données personnelles à être en accord avec la loi (c'est ce que l'on appelle la « mise en conformité »), et protéger le consommateur contre tout usage abusif de données informatiques le concernant.

Pour en savoir plus sur les **missions de la CNIL**, consultez la page dédiée sur leur site Internet.

Le droit à l'image

Chacun d'entre nous est propriétaire de son image et de l'utilisation qui en est faite.

Par « image », on entend ici toute photo ou vidéo sur laquelle vous apparaissez et êtes reconnaissable. En être propriétaire signifie que **personne ne peut conserver ou publier votre image sans votre autorisation**.

Comme souvent, il existe des **exceptions**. Vous ne pouvez pas vous opposer à l'utilisation de votre image si vous apparaissez sur des photos ou vidéos illustrant un **événement d'actualité** ou un **sujet historique**. Ainsi, si son objectif est d'informer, la publication d'images de personnalités publiques est légale, et ces dernières ne peuvent y faire obstacle.

Pour avoir le droit de publier votre photo ou vidéo, le diffuseur (qu'il s'agisse d'un particulier, d'un organisme ou d'une société) doit vous demander votre accord écrit, en précisant **où** et **quand** l'image a été obtenue, ainsi que **l'objectif** pour lequel il souhaite l'utiliser.

De plus, si à l'avenir il souhaitait réutiliser la même image mais dans un **but différent**, il devrait de **nouveau demander** et obtenir votre accord.

Accepter d'**être pris** en photo ou d'être filmé ne signifie pas pour autant que vous êtes d'accord pour que l'image soit **diffusée** : les **2 consentements sont indépendants** l'un de l'autre.

Par conséquent, s'il vous arrivait un jour de vous reconnaître dans une photo ou vidéo publiée sur Internet alors même que vous n'avez pas donné votre accord écrit pour cela, vous seriez en droit d'exiger et d'obtenir la suppression de cette image.

En résumé

- **Faites attention lorsque vous publiez** des photos, vidéos, messages ou commentaires sur Internet ; ayez conscience qu'une fois publiés, le risque existe qu'ils échappent à votre contrôle.
- Modifiez les **paramètres de confidentialité** de vos comptes sur les réseaux sociaux pour en restreindre l'accès à vos seuls amis.
- Le **droit à l'oubli** vous permet de :
    - demander la **suppression de données personnelles** préjudiciables, en vous adressant aux responsables des sites qui les ont publiées ;
    - demander le **déréférencement** de résultats de recherches vous concernant, en utilisant les formulaires en ligne mis à votre disposition par les moteurs de recherche.
- Le **droit à l'image** établit que nul ne peut conserver, utiliser ou publier des photos ou vidéos sur lesquelles vous apparaissez, sans votre accord écrit.

- Pour toute question concernant vos droits ou en cas de problème lié au traitement de vos données personnelles, vous pouvez vous adresser à la **CNIL** (Commission nationale informatique et libertés), organisme public chargé de vous informer et de vous protéger.

Chiffrez vos données si nécessaire

Que ce soit dans notre activité professionnelle ou dans un cadre privé, nous possédons et utilisons un nombre sans cesse croissant de données. Celles que nous conservons au regard de notre travail sont sous notre responsabilité ; il nous incombe donc de ne pas mettre en péril leur sécurité.

Le stockage dans le Cloud ou sur un serveur

La majorité des entreprises stockent leurs données dans le **Cloud** : les données sont alors enregistrées via Internet sur des serveurs éloignés géographiquement ; plusieurs copies sont réalisées, de manière à mieux protéger la sauvegarde. Grâce à l'existence de copies, si l'un des serveurs rencontrait un problème, les données ne seraient pas perdues pour autant.

Toutefois, certaines font le choix de sauvegarder leurs fichiers sur des **serveurs** (sorte d'ordinateur super puissant offrant beaucoup plus d'espace de stockage qu'un ordinateur de bureau) situés dans leurs propres locaux.

> Par défaut, les données ainsi sauvegardées, que ce soit dans le Cloud ou sur des serveurs, le sont sous forme de texte brut ; cela signifie que leur stockage n'est pas sécurisé.

Si une personne mal intentionnée réussissait à y accéder, elle n'aurait alors aucune difficulté à les lire ou à les copier. Or, il est essentiel d'assurer la sécurité et la confidentialité des fichiers d'ordre professionnel.

Différenciez vos documents professionnels des personnels

La première règle de prudence à adopter est de séparer vos données personnelles de vos données professionnelles. Ainsi, il est fortement déconseillé de sauvegarder des données professionnelles sur des supports personnels (clé USB ou ordinateur portable). De même qu'il vaut mieux éviter de connecter une clé USB privée aux ordinateurs de l'entreprise.

Tout ceci afin d'éviter un phénomène de **piratage en cascade** : si par malheur vous étiez victime d'un piratage, le fait de brancher votre clé USB personnelle sur les machines de votre entreprise risquerait de permettre la propagation du virus.

Veillez au stockage sur portable ou clé USB

Imaginez un instant que vous ayez copié une partie de vos données sur une clé USB et que vous ayez malencontreusement égaré celle-ci… **Toute personne qui trouvera votre clé aura accès à vos fichiers et se retrouvera donc en**

possession de vos données personnelles. Il ne reste alors plus qu'à souhaiter que cette personne ne soit pas mal intentionnée…

Les données stockées sur un **ordinateur** sont elles aussi **exposées aux risques**, de même que les **courriers** que vous échangez avec votre entourage ou vos collègues : entre votre boîte d'envoi et la boîte de réception du destinataire, un e-mail passe en effet par plusieurs étapes intermédiaires (ou serveurs) et peut être lu par d'autres personnes que celle à laquelle il était destiné.

Quand bien même vos échanges n'auraient rien de confidentiel, vous ne souhaitez sûrement pas pour autant que n'importe qui puisse lire les mails que vous échangez avec vos proches ou vos collègues de travail !

> Le **chiffrement des données** permet d'assurer leur **sécurité** et par là même, leur **confidentialité**.

Cela consiste à coder les données de telle sorte qu'elles ne puissent être lues que par celui qui possède la **clé du code**. Les données chiffrées peuvent ainsi être protégées lorsqu'elles sont stockées sur un support, mais aussi pendant les divers transferts dont elles peuvent être l'objet (envoi de mails et pièces jointes, téléchargement de documents).

> En plus de garantir la confidentialité de nos données et de nos communications, le chiffrement permet également d'assurer l'authenticité et l'intégrité des e-mails : ainsi, si vous êtes le destinataire d'un mail chiffré, vous pouvez être certain qu'il provient bien de l'expéditeur « officiel » (et pas d'un usurpateur), et qu'il n'a pas été modifié par un tiers avant d'arriver dans votre boîte de réception.

Comment chiffrer ses fichiers, répertoires et courriers ?

> Il existe 2 principales méthodes de chiffrement : symétrique ou asymétrique.

Avec un **chiffrement symétrique**, il n'y a qu'**une seule et même clé** utilisée pour chiffrer le code puis pour le déchiffrer. Si vous cryptez un fichier à l'aide de cette méthode avant de l'envoyer à un collègue, par exemple, vous devrez transmettre la clé à votre collègue afin qu'il puisse accéder au fichier.

De son côté, le **chiffrement asymétrique** utilise **2 clés** : une première pour **chiffrer** les données, une seconde pour les **déchiffrer**. La seconde clé est une clé privée (que vous ne devez donc communiquer à personne), tandis que la première est publique et doit au contraire être transmise au destinataire du mail ou du fichier. La confidentialité de ce dernier est ainsi garantie : il ne pourra en effet être lu que par la personne qui possède la clé publique correspondant à la clé privée utilisée par l'expéditeur.

Si le chiffrement asymétrique est davantage utilisé dans le monde de l'entreprise, le chiffrement symétrique, plus rapide et simple à mettre en œuvre, s'avère plus répandu chez les particuliers.

Exemples de logiciels de chiffrage

Il existe de nombreux logiciels de chiffrement symétrique que l'on peut facilement télécharger sur Internet.

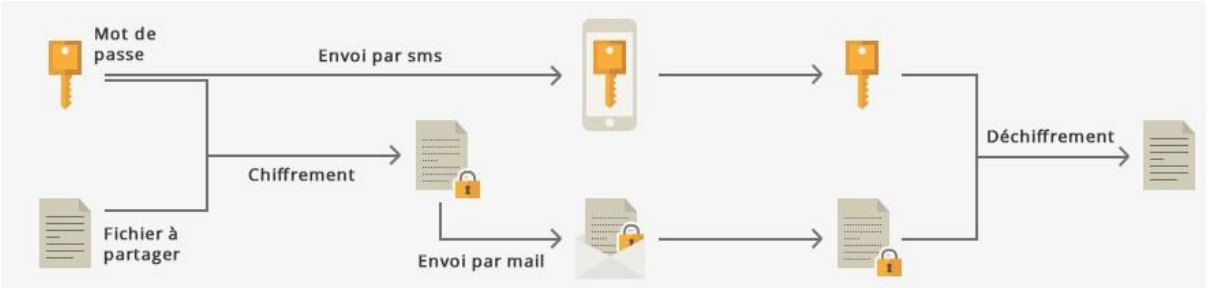
Chiffrer les courriels est toutefois un peu plus ardu à réaliser et nécessite d'adopter un chiffrement asymétrique (on ne trouve en effet sur le web aucun logiciel permettant de crypter un mail et utilisant le codage symétrique).

Prenons un exemple pour comprendre comment chiffrer un fichier :

Laurent souhaite envoyer à sa fiancée un fichier qu'il juge confidentiel.
Il procède au chiffrement du fichier concerné avant de rédiger son mail et d'y ajouter le fichier en pièce jointe. Puis il l'envoie à Mélanie (sa fiancée).
Immédiatement après avoir cliqué sur le bouton « *Envoyer* » de sa messagerie, il prend son téléphone et transmet à Mélanie par SMS le code de déchiffrement (ou *clé*).

En cas de piratage, le fichier demeure susceptible d'être intercepté mais même alors, il ne sera d'aucune utilité au pirate. S'il tente de lire le contenu du fichier, ce dernier ne verra en effet qu'une suite de caractères (chiffres, lettres et symboles mélangés) totalement incompréhensible.

Seule Mélanie, qui est en possession de la clé de déchiffrement, sera apte à redonner au fichier son apparence initiale ; ainsi, elle sera l'unique personne à pouvoir le lire.



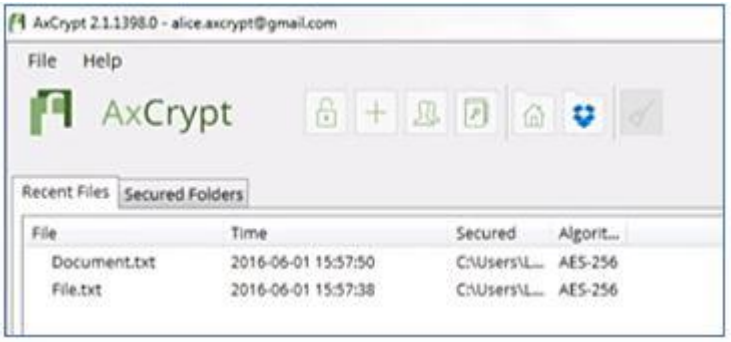
Source : cnil.fr

Parmi les nombreux logiciels disponibles, la CNIL conseille notamment l'utilisation d'**AxCrypt** ou de **7-Zip**.
Ils sont tous les 2 **gratuits** et relativement faciles à utiliser.

Utilisez AxCrypt

Une fois installé, il sera très facile de chiffrer fichiers et répertoires. Notez que si vous souhaitez crypter plusieurs fichiers, le plus rapide sera alors de les placer dans un même répertoire puis de chiffrer ce dernier, car le chiffrement d'un répertoire entraîne celui de tous les fichiers qu'il contient.

- Démarrez **AxCrypt**.
- Cliquez sur le bouton **+** dans la fenêtre du logiciel.
- Choisissez les fichiers ou dossiers à chiffrer,
  ou glissez et déposez des fichiers ou dossiers dans la fenêtre **AxCrypt**
  (vous pouvez aussi simplement faire un clic droit sur un fichier ou dossier dans votre explorateur de fichiers, puis cliquer sur la commande **AxCrypt** du menu contextuel).
- C'est fait ! Ils sont maintenant sécurisés : leur icône s'est transformée pour afficher le logo **AxCrypt** (cadenas blanc sur fond vert).



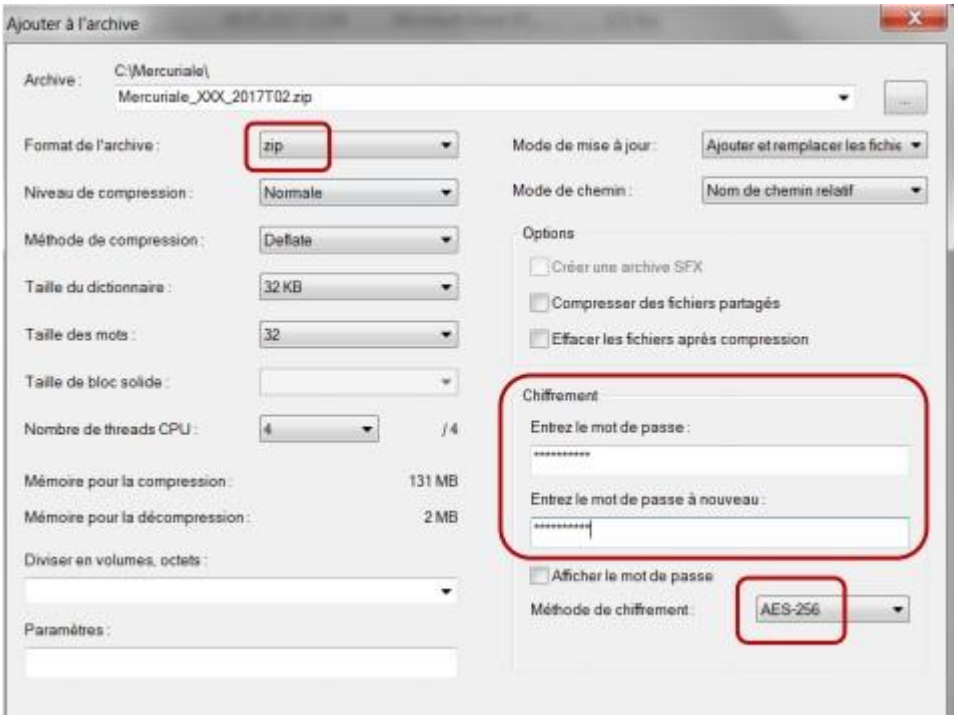
Écran d'AxCrypt

Utilisez 7-Zip

Ce logiciel, souvent utilisé pour compresser des fichiers trop volumineux, permet également de les chiffrer.

Une fois que vous aurez téléchargé et installé **7-Zip**, vous devrez démarrer le logiciel puis sélectionner le fichier ou dossier à chiffrer. Vous pouvez également faire un clic droit sur un fichier ou dossier dans votre explorateur et choisir **7-Zip** > **Ajouter à l'archive**.

Dans la fenêtre qui s'affiche à l'écran, vérifiez que la méthode de chiffrement est ***AES*** puis entrez un mot de passe de votre choix dans la rubrique **Chiffrement**.



Écran de 7-Zip

Le fichier chiffré sera placé dans le même répertoire que le fichier d'origine.

> Quel que soit le logiciel utilisé, si vous souhaitez envoyer des fichiers chiffrés à un destinataire, ce dernier ne pourra les lire que s'il est lui aussi équipé du même logiciel.

> Dans le cas de **7-Zip**, vous devrez en outre lui communiquer le mot de passe que vous aurez choisi lors du chiffrement.

Chiffrez vos e-mails

Comme je vous le disais précédemment, **chiffrer vos e-mails** ne sera malheureusement pas aussi facile. Mais voici toutefois 2 méthodes assez simples, incluant néanmoins quelques contraintes.

> Le chiffrement de mails ne peut être réalisé que si vous utilisez un logiciel de messagerie tel **Microsoft Outlook** ou **Mozilla Thunderbird**.

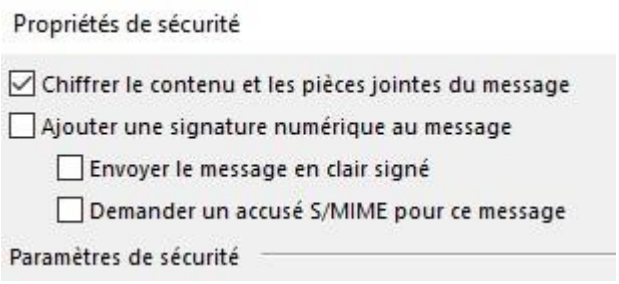
Chiffrez avec un logiciel de messagerie

Si vous possédez **Microsoft Outlook** et bénéficiez d'un abonnement **Office 365**, la procédure est très simple :

1. Dans la fenêtre Nouveau message, sous l'onglet **Options**, cliquez sur *le* ***lanceur de boîte de dialogues*** du groupe **Autres Options**.

Écran Microsoft Outlook

2. Cliquez ensuite sur ***Paramètres de sécurité*** et puis cochez la case **« Chiffrer le contenu et les pièces jointes du messages »**.



Propriétés de sécurité sur Microsoft Outlook

3. Rédigez votre message puis cliquez sur ***Envoyer***.

> Vous pouvez aussi paramétrer **Outlook** de manière à chiffrer absolument tous les messages que vous enverrez.

1. Sous l'onglet ***Fichier***, cliquez sur ***Options*** puis sur ***Centre de gestion de la confidentialité*** et enfin sur ***Paramètres du centre de gestion de la confidentialité***.

2. Sous l'onglet ***Sécurité de messagerie électronique***, sous ***Courrier électronique chiffré***, cochez la case ***Chiffrer le contenu des messages et des pièces jointes pour les messages sortants***.

Chiffrez avec le logiciel Thunderbird

1. Téléchargez le logiciel gratuit Thunderbird puis suivez les instructions d'installation.

2. Téléchargez Gpg4win. C'est ce logiciel qui permettra le chiffrement (et déchiffrement) de vos mails.

3. Installez Enigmail, (sorte de complément à *Thunderbird*, nécessaire pour que celui-ci puisse « travailler » avec *Gpg4win*).

Pour l'installer, démarrez **Thunderbird** puis cliquez sur le menu **Outils** et sur **Modules complémentaires**. Un nouvel onglet apparaît : tapez ***Enigmail*** dans la zone de recherche et lancez le téléchargement.

Lorsque les 3 programmes auront été installés et que vous aurez paramétré Thunderbird avec votre compte de messagerie (Menu Fichier > Nouveau > Compte courrier existant), vous devrez alors créer vos **clés cryptographiques** : une première clé privée que vous ne devrez communiquer à personne, ainsi qu'une seconde clé publique que vous transmettrez aux destinataires de vos mails.

- Cliquez dans le menu **Enigmail** et sélectionnez **Assistant de configuration**.
- Choisissez l'option : « *Je préfère la configuration standard* ».
- Cliquez sur **Suivant** et cochez « *Je veux créer une nouvelle paire de clefs pour signer et chiffrer mes messages* ».
- Cliquez de nouveau sur **Suivant**.
- Tapez le mot de passe de votre choix puis sélectionnez votre compte mail (pour le rattacher à vos clés cryptographiques).

Les clés ont été créées !

Pensez ensuite à envoyer un message aux destinataires concernés afin de leur transmettre votre clé publique. Pour cela, cliquez sur le bouton **Attacher ma clé publique** dans la fenêtre **Nouveau message** avant de cliquer sur **Envoyer**.

Il est ensuite très simple de chiffrer un mail, puisqu'il suffit pour cela **de cocher la case** affichant un **cadenas** de la fenêtre **Nouveau message** avant de cliquer sur **Envoyer**.

Le destinataire d'un mail chiffré et envoyé avec **Thunderbird** devra, pour le lire, être lui aussi équipé des 3 mêmes logiciels et posséder en outre la clé publique de l'expéditeur.

En résumé

- **Distinguez** bien les données personnelles des données professionnelles.
- Le **chiffrement** des données est une technique qui permet de garantir leur confidentialité et leur intégrité.
- Une fois chiffrées, les données deviennent **illisibles** et seule la personne qui possède la **clé du code** peut les consulter.
- Pour chiffrer vos fichiers et répertoires, privilégiez l'un des 2 logiciels suivants : **AxCrypt** ou **7-Zip**.
- Pour chiffrer vos courriels, vous aurez besoin de **Microsoft Outlook** assorti d'un abonnement Office 365 (payant) ou de **Thunderbird**, GPGWin4 et Enigmail (gratuits).

Protégez votre ordinateur

Installez un antivirus

Un virus informatique (également appelé *malware*) est un programme conçu pour se répliquer et se transmettre automatiquement à d'autres ordinateurs.

Les virus sont dissimulés dans d'autres logiciels, également dans des fichiers ou des e-mails, ou encore dans une page Internet. Ils peuvent aussi être véhiculés par une clé USB ou une carte mémoire (contenant un fichier infecté).

En fonction du type de virus, il agira différemment, mais dans tous les cas il perturbera le **fonctionnement de l'ordinateur** infecté : du simple ralentissement à la mise hors service de l'ordinateur, en passant par l'impossibilité d'ouvrir des fichiers, d'utiliser des applications ou encore de surfer sur Internet, tout est possible.

Les virus rendent vos données illisibles ou les supprime purement et simplement.

Certains virus, appelés ***Chevaux de Troie***, permettent aux pirates de prendre, à distance, le contrôle de votre machine. Outre qu'ils ont alors la possibilité de dérober vos données personnelles, ils peuvent également utiliser votre messagerie ou se servir de votre ordinateur pour infecter d'autres ordinateurs.

D'autres, nommés **logiciels espions** ou **Spywares**, vont espionner tout ce que vous faites : les applications que vous utilisez, les sites Internet vous visitez, les mails que vous envoyez. Ils surveillent tout et enregistrent même parfois ce que vous tapez au clavier.

Ils ont donc accès à toutes vos données personnelles, dont vos mots de passe et coordonnées bancaires.

Vous avez peut-être entendu parler ces dernières années dans les médias d'un autre type de virus : les ***ransomwares***. Ces derniers chiffrent toutes les données présentes sur l'ordinateur infecté, puis exigent une rançon en échange de la clé qui permettra de les déchiffrer et de les rendre de nouveau accessibles.

Protégez-vous des virus

Tout ordinateur, qu'il s'agisse d'un matériel professionnel ou privé, devrait être équipé d'un **antivirus** : c'est une mesure de sécurité basique et fondamentale.

Un **antivirus** est un logiciel qui, comme son nom l'indique, est conçu pour détecter & éliminer les virus. Il analyse l'ensemble des fichiers et programmes déjà présents sur l'ordinateur, mais aussi tout contenu téléchargé ou transmis par courriel. S'il détecte un virus, il bloque immédiatement l'action de ce dernier avant de le supprimer.

S'ils sont indispensables à votre sécurité, les logiciels antivirus **n'offrent toutefois pas une protection absolue**. Ils vous protégeront très efficacement contre les virus les plus connus mais peuvent être **impuissants face à un virus tout récemment créé**.

Le respect de quelques précautions vous aidera à parfaire la protection de votre antivirus :

Connectez-vous sur un compte utilisateur

Il existe 2 grands types de compte sur un ordinateur :

- le compte **utilisateur** ; à privilégier. Il convient parfaitement pour votre **usage courant** (naviguer sur Internet, échanger des courriels, utiliser vos logiciels, etc.) ;
- le compte **administrateur** ; nécessaire seulement pour intervenir sur le fonctionnement global de la machine (par exemple, créer un nouveau compte utilisateur ou installer un nouveau logiciel ou périphérique).

Si vous cliquez sur un lien frauduleux alors que vous êtes connecté en tant qu'administrateur, un pirate qui accèderait alors à votre machine aurait la possibilité de désactiver votre antivirus (l'ordinateur serait alors totalement vulnérable). Si au contraire, vous utilisez un compte utilisateur, le pirate échouera à désactiver l'antivirus, car il n'aura pas les autorisations nécessaires.

Téléchargez en sécurité

Lorsque vous téléchargez des fichiers ou des logiciels, **vérifiez la fiabilité du site** sur lequel vous effectuez le téléchargement, sans quoi vous vous exposez à télécharger des fichiers porteurs de virus. En cas de doute, n'hésitez pas à changer de site.

Pour télécharger un **logiciel**, il est recommandé de se rendre sur le **site de son éditeur**.

Lors d'un téléchargement, pensez également à **décocher** toutes les cases générant l'installation de **programmes complémentaires**.

Enfin, avant d'ouvrir vos fichiers téléchargés, faites-les **analyser** par votre **antivirus**.

Choisissez votre antivirus

Un bon antivirus :

- efficace dans la **détection des menaces** ;
- **facile à installer** et à utiliser ;
- ne doit pas altérer par son fonctionnement les performances de votre ordinateur ;
- doit générer le moins possible de « *faux positifs* ».

> Lorsque qu'un antivirus vous alerte en indiquant avoir détecté une menace alors que vous venez par exemple d'installer un nouveau logiciel tout à fait inoffensif, il s'agit d'une erreur de détection qu'on appelle *faux positif*. De même, s'il vous interdit l'accès à un site Internet de confiance parce qu'il a cru détecter un élément frauduleux.

Voici quelques antivirus connus qui satisfont à tous ces critères :

- Avast (gratuit) ;
- BitDefender (environ 29€99) ;
- AVG (gratuit) ;
- Avira (gratuit) ;
- Malwarebytes (gratuit).

> Pourquoi choisir un antivirus payant si les gratuits satisfont également aux critères ?

Les antivirus offrent une **même qualité de protection** qu'ils soient gratuits ou payants ; la différence réside souvent dans des **services complémentaires**. Les antivirus gratuits existent d'ailleurs quasiment tous dans une version payante qui offre des fonctionnalités supplémentaires, telles qu'un **gestionnaire de mots de passe** ou un **pare-feu**.

Installez et configurez votre antivirus Avast

Pour télécharger l'un d'entre eux, rendez-vous sur le site indiqué puis suivez les instructions de téléchargement et d'installation. Une fois l'installation terminée, l'antivirus démarre automatiquement et fonctionnera désormais en « tâche de fond » : votre ordinateur est protégé.

À titre d'information, nous décrivons ci-dessous plus en détail la procédure à suivre pour installer et configurer l'antivirus **Avast** :

- rendez-vous sur le site avast.com pour télécharger le logiciel ;

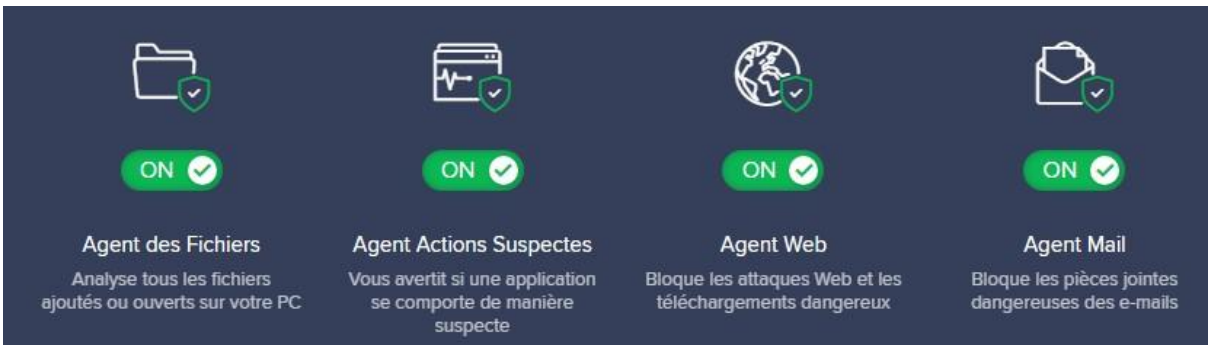
- double-cliquez ensuite sur le fichier apparaissant en bas à gauche de votre écran (ou dans votre dossier *Téléchargements*) et répondez *Oui* au message qui s'affiche ;
- suivez simplement les instructions d'installation

Une fois celle-ci achevée, Avast est en fonctionnement et protège votre ordinateur.

L'icône Avast apparaît dans votre **zone de notification** (tout en bas à droite de votre écran).

Par défaut, les fonctionnalités importantes (analyse de fichiers, surveillance des téléchargements et des e-mails) qui assurent votre protection sont activées.

Pour le vérifier, ouvrez d'abord l'interface du logiciel en cliquant sur son icône dans la zone de notification. Cliquez ensuite sur **Protection** dans le volet gauche de la fenêtre **Avast** puis sur **Agents principaux**.



Écran des agents principaux Avast

Pour accroître encore votre sécurité, vous pouvez configurer Avast de façon à ce qu'il **analyse automatiquement** le contenu de votre ordinateur à chaque démarrage :

- cliquez dans le volet gauche sur **Protection** puis à droite sur **Recherche de virus** ;

Cliquez ensuite sur le bouton Ouvrir de la rubrique Scan au démarrage

- cliquez sur **Exécuter au prochain redémarrage du PC**.

L'installation d'un antivirus est essentielle à la sécurité de votre ordinateur, mais ne vous garantit pas qu'il sera à 100 % invulnérable. Des protections complémentaires sont également recommandées.

Ajoutez des protections complémentaires

Utilisez un bloqueur de fenêtres contextuelles

Quel que soit le navigateur Internet que vous avez coutume d'utiliser, ce dernier est équipé d'un **bloqueur de fenêtres contextuelles**, aussi appelé **bloqueur de pop-up**.

Les fenêtres contextuelles (ou *pop-up*) sont des fenêtres (publicitaires dans la majorité des cas) qui apparaissent soudainement à l'écran pendant que vous surfez sur Internet, sans que vous ne l'ayez ni souhaité ni approuvé.

Sur certains sites, elles peuvent être relativement fréquentes et gêner votre navigation. Il est donc recommandé de **paramétrer votre navigateur** de façon à **empêcher l'affichage intempestif** de ces fenêtres.

Les pop-ups peuvent aussi quelquefois servir de supports à des techniques de **phishing** (sous la forme par exemple d'une annonce publicitaire vous avertissant que vous êtes l'heureux gagnant d'un smartphone et qu'il suffit de cliquer pour valider votre gain.

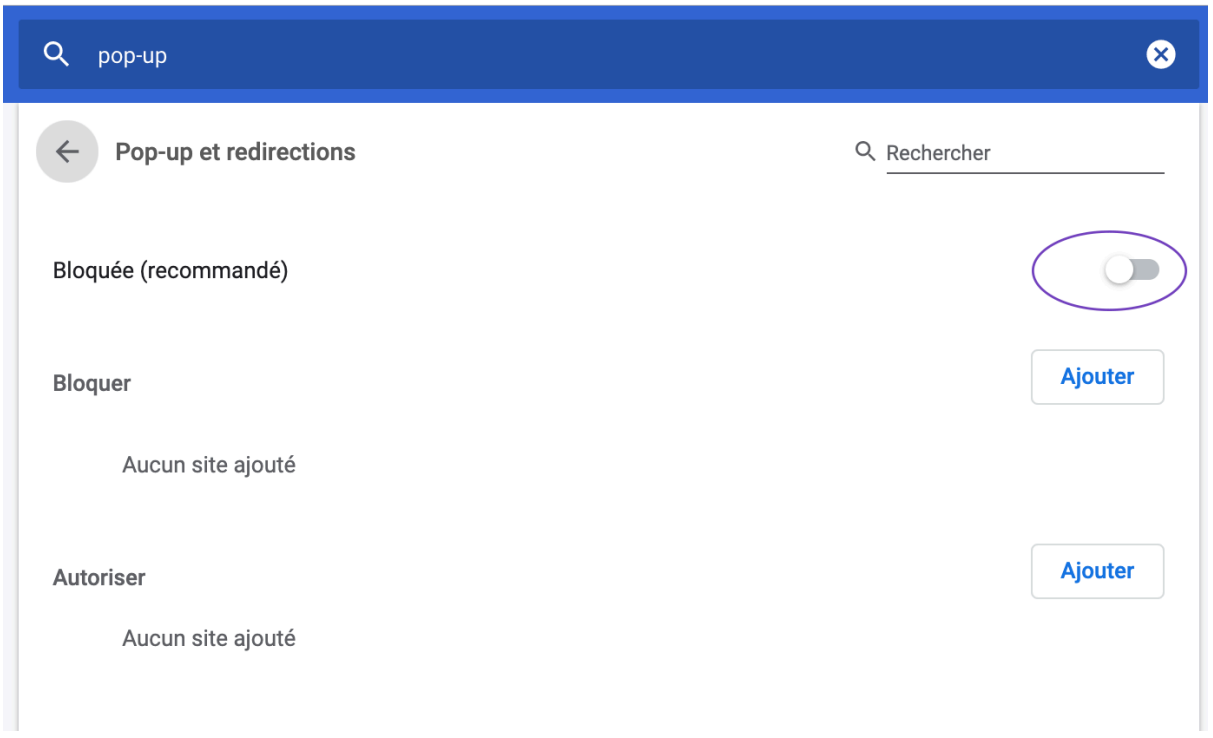
Loin de gagner quoi que ce soit, vous risquez fort de vous faire **dérober des données personnelles** ou véhiculer des **virus**, lorsqu'il vous sera proposé de

télécharger gratuitement un logiciel utilitaire, dans lequel se cache un programme malveillant).

Toutefois, il peut arriver que les fenêtres contextuelles soient **indispensables au bon fonctionnement d'un site** : c'est par exemple le cas pour les sites de banque en ligne. La solution, dans ce cas, est d'**indiquer à votre navigateur** que vous **autorisez** les fenêtres contextuelles de ce **site en particulier**. Il bloquera alors toutes les fenêtres contextuelles sauf celles du ou des sites que vous aurez autorisé(s).

Bloquez des pop-ups sur Google Chrome

- Cliquez sur le bouton **Menu** en haut à droite de votre écran puis sur **Paramètres**.
- Tapez dans la **barre de recherche « pop-up »**.
- Cliquez, comme indiqué via votre recherche, sur **Paramètres du site**.
- Cliquez sur la rubrique **Pop-up et redirections**.



Cliquez sur le bouton poussoir à droite pour activer le blocage des pop-ups

- Pour autoriser les fenêtres contextuelles provenant d'un site en particulier, cliquer sur le bouton **Ajouter** dans la rubrique **Autoriser** puis tapez l'adresse du site concerné et cliquez sur **Ajouter**.

Avec Microsoft Edge

- Cliquez sur le bouton **Menu**  en haut à droite de votre écran puis sur **Paramètres**.
- Cliquez sur **Confidentialité et sécurité.**

Cliquez sur le bouton poussoir pour activer le blocage des fenêtres contextuelles

Microsoft Edge ne permet pas d'autoriser les fenêtres contextuelles pour un site en particulier.

Avec Mozilla Firefox

- Cliquez le bouton **Menu**  puis sur **Options**.
- Cliquez sur l'onglet **Confidentialité et sécurité**.
- Dans la rubrique **Autorisations**, cochez la case **Activer le bloqueur de fenêtres**.
- Pour autoriser les fenêtres d'un site en particulier, cliquez sur le bouton **Exceptions.**
- Tapez l'adresse du site concerné puis cliquez sur **Autoriser.**

Avec Safari

- Dans le menu **Safari**, cliquez sur **Préférences**.
- Cliquez sur **Sécurité**.
- Cochez la case **Bloquer les fenêtres surgissantes**.

Utilisez un pare-feu

Dès qu'il est connecté à un réseau (professionnel ou privé) ou à Internet, un ordinateur est exposé à des tentatives d'intrusion.

Un pare-feu, ou ***firewall*** en anglais, est un logiciel conçu pour détecter et empêcher d'éventuelles tentatives d'intrusion. Chaque fois qu'une application souhaite se connecter à Internet ou à n'importe quel réseau (à celui d'une entreprise, par exemple), **le pare-feu autorise ou refuse la connexion**.

De même, lorsqu'une application provenant d'Internet ou d'un réseau tente de se connecter à votre ordinateur (ce qui est par exemple le cas lorsque vous

téléchargez puis installez un programme depuis le web), le pare-feu va approuver ou interdire la connexion.

Sans pare-feu, votre ordinateur ressemble, pour un pirate, à une maison dont la porte d'entrée serait constamment ouverte (un peu trop tentant pour les cambrioleurs ! )

Si un logiciel antivirus constitue une bonne protection et permet de détecter les virus présents ou entrants, l'installation d'un **pare-feu** permettra de **renforcer votre sécurité** en empêchant les pirates de s'introduire dans votre ordinateur et de dérober vos données personnelles.

Choisissez et installez votre pare-feu

Comme pour un antivirus, il n'est pas nécessaire d'acheter un pare-feu pour être bien protégé ; les **pares-feux gratuits sont en effet tout aussi efficaces que les payants**. Là encore, les différences de prix s'expliquent par des fonctionnalités supplémentaires.

Il existe de nombreux pares-feux payants ou gratuits disponibles sur Internet :

- **ZoneAlarm**

Pare-feu très répandu et utilisé par de nombreux internautes depuis plus de 15 ans. Bien que complet et fort efficace, son interface peu intuitive ne convient pas à tous les utilisateurs ;

- **Comodo**

Également reconnu depuis plusieurs années pour son efficacité, ce logiciel simple à utiliser offre un excellent niveau de sécurité. Son interface est plus simple, voici comment l'installer.

1. Télécharger Comodo, via ce lien.

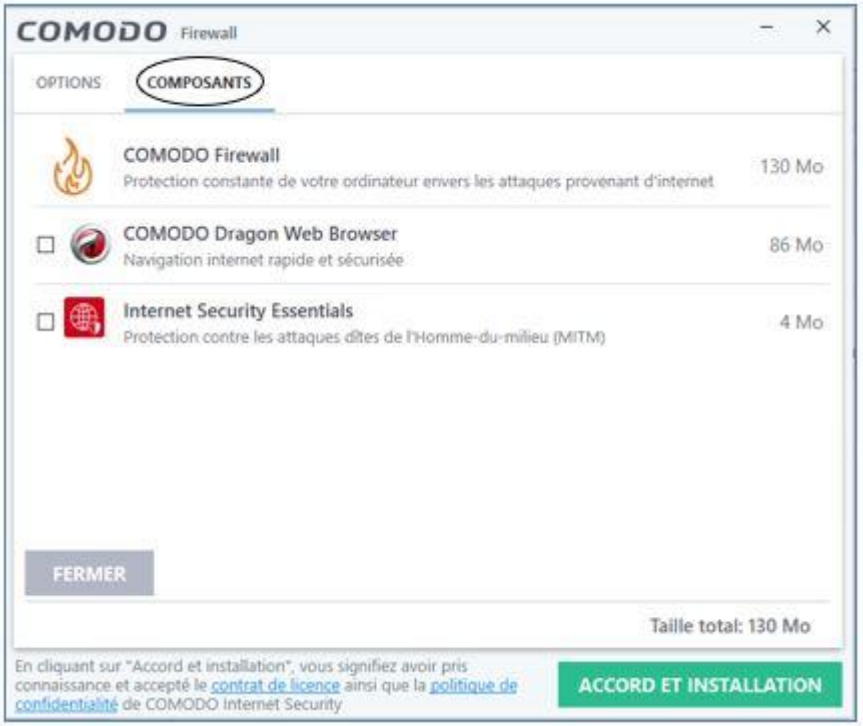
2. Double-cliquez ensuite sur le fichier qui apparaît en bas à gauche de votre écran ou dans votre dossier ***Téléchargements***.

Fréquemment, lorsque vous installez un logiciel, celui-ci tente de vous **pousser à installer d'autres programmes** provenant du même éditeur.

Comodo n'échappe pas à la règle et propose, parallèlement à l'installation de son pare-feu, 2 autres logiciels : un navigateur Internet et un utilitaire de sécurité : ils ne sont absolument pas nécessaires.

Pour éviter leur installation, dans la première fenêtre affichée par **Comodo** :

3. Cliquez sur le bouton Options puis sur l'onglet Composants.

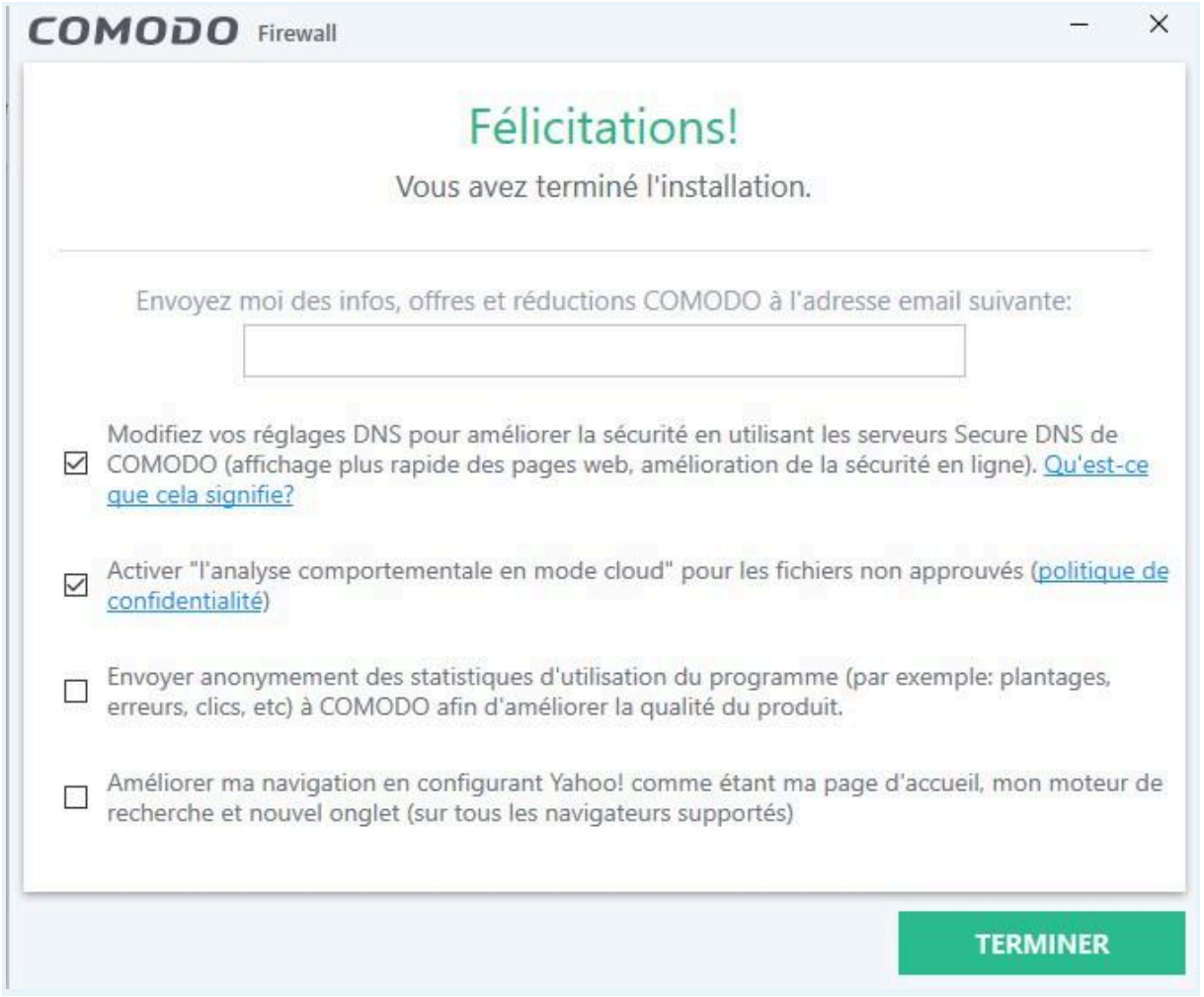


4. Décochez les cases COMODO Dragon Web Browser et Internet Sécurity Essentials.

5. Cliquez sur le bouton **FERMER**.

6. Cliquez sur le bouton **ACCORD ET INSTALLATION**.

Comodo affiche une dernière fenêtre pour vous indiquer que l'installation est terminée.
Plusieurs options y sont proposées :



Les différentes options proposées par Comodo

Comprendre les options proposées

Première option, « *Modifier vos réglages DNS pour améliorer la sécurité en utilisant les serveurs Secure DNS de Comodo* » :

DNS signifie ***Domaine Name Server*** *ou,* en français, ***Système de Nom de Domaine***.
L'adresse d'un site Internet se compose d'un préfixe (*www*) suivi d'un nom de domaine.
Par exemple, **openclassrooms.com** est un nom de domaine.

Mais pour se rendre sur un site Internet, le nom du domaine ne suffit pas. Les ordinateurs ont en effet besoin de connaître l'adresse IP correspondante (suite de chiffres permettant d'identifier de manière unique chaque machine reliée à Internet).

Demander à votre ordinateur de se rendre sur un site s'il connaît uniquement son nom de domaine et non son adresse IP, c'est exactement comme si vous deviez vous rendre chez M. Henri Lafont, alors que ce dernier ne vous a fourni que son nom, mais pas son adresse !

Un serveur DNS permet de faire le lien entre un domaine et son adresse IP.

Ainsi, si vous souhaitez visiter le site www.openclassrooms.com, votre navigateur Internet va envoyer une demande au serveur DNS utilisé par votre ordinateur ; le serveur DNS lui renverra en retour l'adresse IP correspondante.

En général, le serveur DNS qu'utilise votre ordinateur est celui de votre fournisseur d'accès (Orange, Free ou SFR, par exemple). Vous pouvez bien entendu décocher la case ; toutefois, il est **conseillé de conserver cette option** : l'utilisation des serveurs DNS de Comodo rendra votre navigation plus rapide et encore plus sécurisée.

Seconde option *: « Activer l'analyse comportementale en mode cloud pour les fichiers non approuvés »* :

Cela signifie que tout fichier inconnu sera envoyé au serveur Comodo pour une analyse : il sera testé afin de savoir s'il s'agit ou non d'un fichier malveillant. Votre ordinateur recevra quelques minutes plus tard le résultat de cette analyse et vous alertera en cas de danger.

Troisième option : *« Envoyer anonymement des statistiques d'utilisation du programme » :*

Cette option, commune à un grand nombre de logiciels, permet à leurs éditeurs d'établir des statistiques sur l'utilisation de leurs produits.

À vous de voir si vous souhaitez la désactiver ou non.

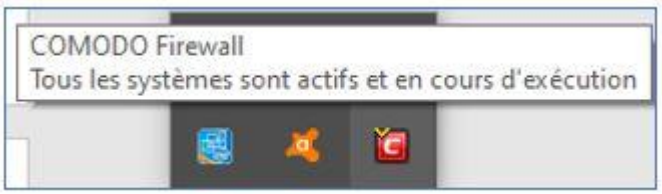
Quatrième option *: « Améliorer ma navigation en configurant Yahoo ! comme étant ma page d'accueil, mon moteur de recherches et nouvel onglet » :*

Décochez cette case afin de conserver vos moteurs de recherches et page d'accueil habituels.

7. Vous pouvez maintenant cliquer sur **Terminer** ! 

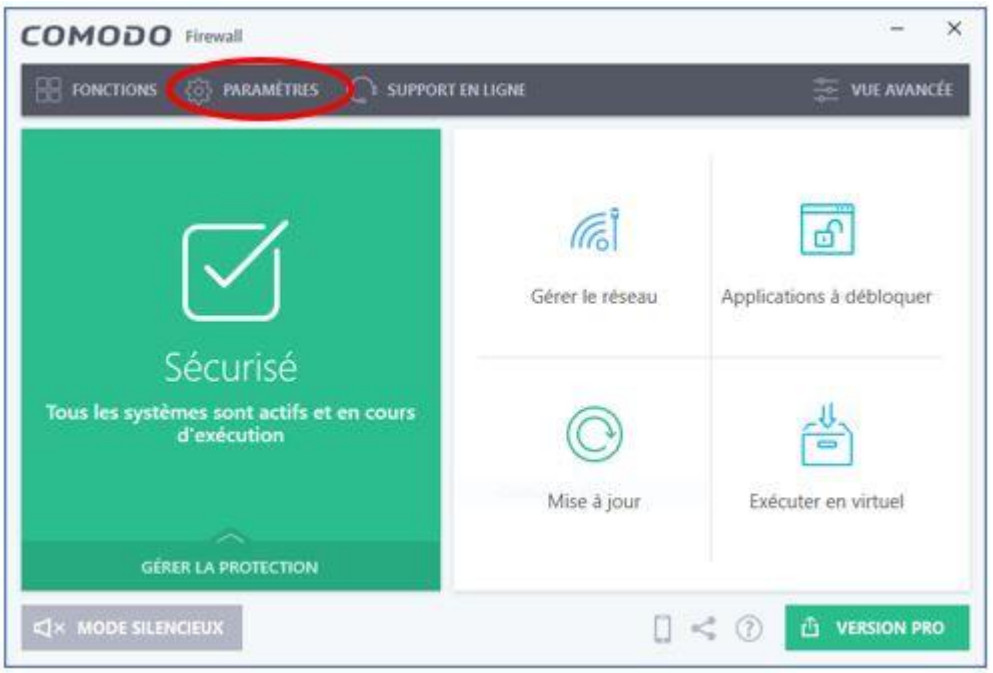
8. Comodo indique qu'il doit redémarrer l'ordinateur pour finaliser l'installation : cliquez sur **Redémarrer maintenant**.

Une fois le redémarrage effectué, Comodo est en fonctionnement et protège votre machine des tentatives d'intrusion. Vous pouvez le vérifier en observant l'icône de Comodo (un C blanc sur fond rouge) dans la zone de notification (tout en bas à droite de votre écran) :



L'icône de Comodo

Double-cliquez sur cette icône pour afficher la fenêtre du programme :

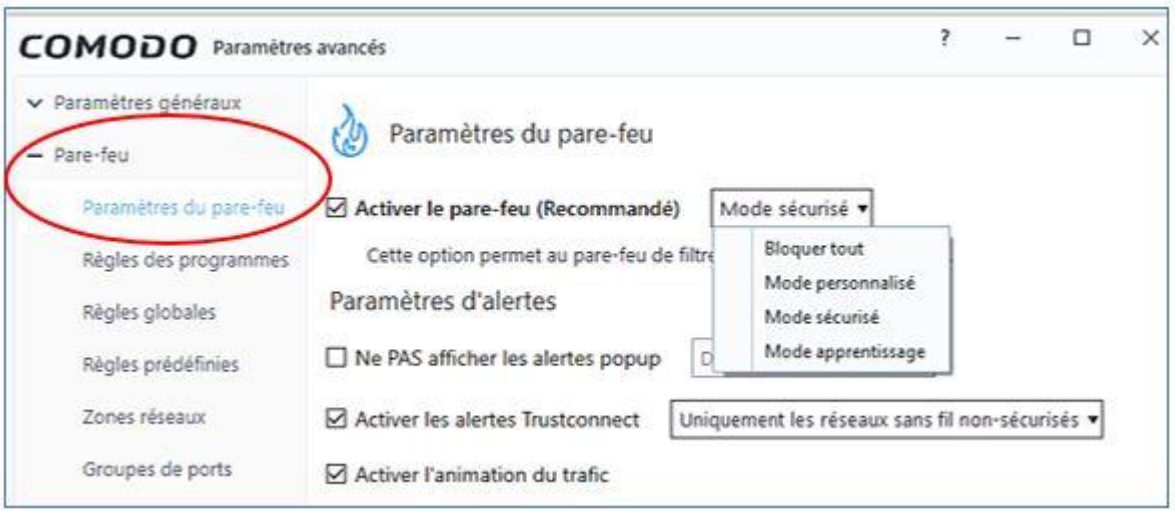


Dashboard des paramètres de Comodo

Par défaut, Comodo fonctionne en mode **sécurisé** ; il est recommandé de conserver ce mode de fonctionnement.

Pour le vérifier :

- cliquez sur ***Paramètres*** en haut à gauche de la fenêtre Comodo ;
- cliquez ensuite dans le volet gauche sur ***Pare-feu*** puis sur ***Paramètres du pare-feu*** :



Dashboard des paramètres du pare-feu

Comprenez le fonctionnement de Comodo

Le pare-feu gérera seul les connexions des applications qu'il conna$it et qu'il sait inoffensives, mais il vous alertera si une application inconnue tente d'établir une connexion.

Supposez par exemple que vous démarriez un jeu vidéo : l'application demande à se connecter à Internet. Comodo affiche un message vous avertissant et demandant si vous autorisez cette connexion. Vous avez alors le choix entre plusieurs options :

Les 3 options suite à une demande d'autorisation de connexion

- **Autoriser** : choisissez cette option si vous êtes certain que l'application est inoffensive.

Par exemple, vous installez un logiciel de traitement de texte tel Microsoft Word ; vous pouvez alors cliquer sur ***Autoriser***.

Si vous cochez la case ***Se souvenir de ma réponse***, Comodo ajoutera le programme à sa liste de programmes approuvés : il autorisera automatiquement toute future tentative de connexion de la part de cette application.

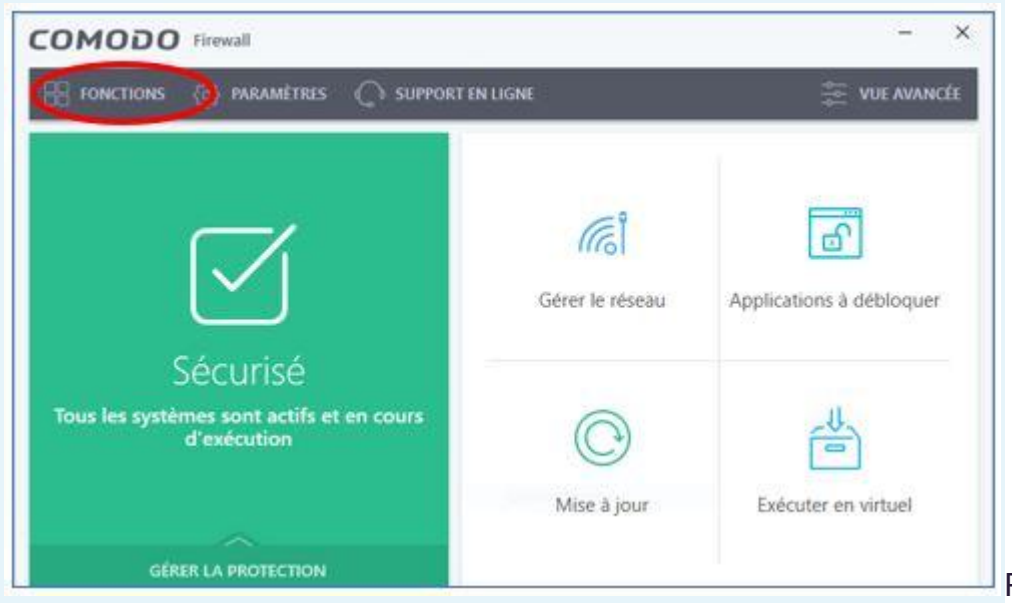
- **Bloquer** : choisissez cette option si ne connaissez pas l'application concernée, si vous pensez avoir affaire à une application malveillante, ou si vous avez des doutes sur sa fiabilité.

Si vous cochez la case ***Se souvenir de ma réponse***, Comodo ajoutera le programme à sa liste d'applications bloquées. Il refusera toute tentative de connexion de la part de cette application sans vous alerter auparavant.

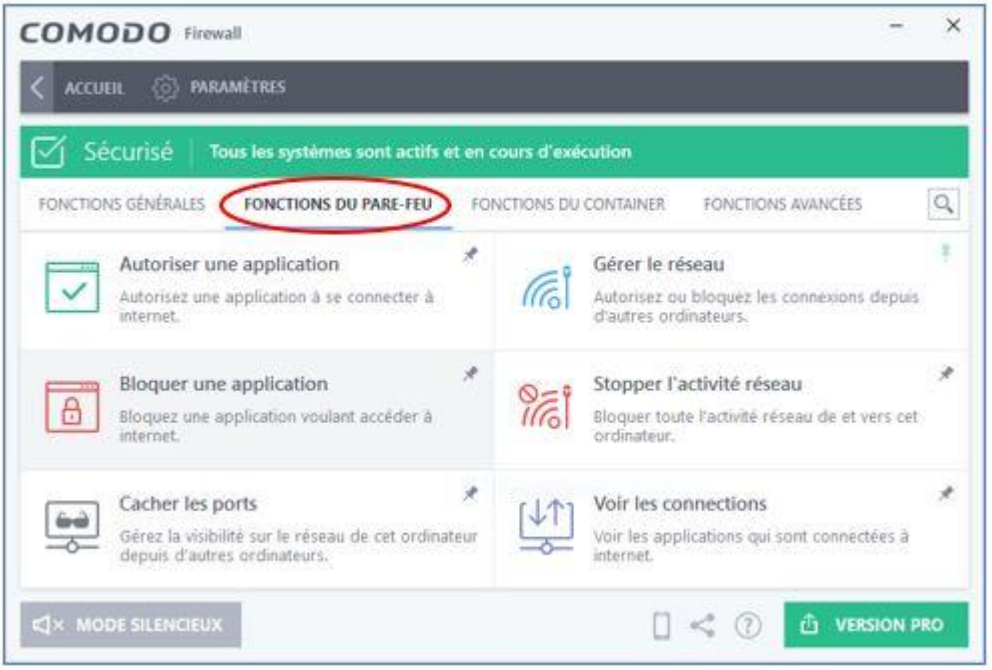
- **Traiter comme :** réservée aux **utilisateurs avancés**, cette option permet un choix personnalisé.

Elle permet par exemple d'autoriser une application présente sur votre ordinateur à envoyer des données vers Internet, tout en lui interdisant de recevoir des informations provenant de l'extérieur.

Vous avez également la possibilité de bloquer ou d'autoriser une application sans attendre que Comodo vous interroge.



Pour cela, cliquez sur Fonctions, en haut à gauche de la fenêtre d'accueil de Comodo



Puis cliquez sur Fonctions du pare-feu

Supposons que vous utilisiez régulièrement un jeu vidéo qui nécessite d'être connecté à Internet.

Vous connaissez ce jeu depuis longtemps et vous êtes absolument certain qu'il ne dissimule aucun programme malveillant. Mieux vaut alors l'ajouter à la liste des applications approuvées, afin que Comodo autorise les connexions de ce programme sans avoir à vous demander chaque fois votre autorisation.

- Cliquez sur ***Autoriser une application***.

Sélectionnez le fichier correspondant au programme dans la fenêtre de l'explorateur de fichiers puis cliquez sur **OK** : c'est fait, le logiciel a été ajouté à la liste des applications approuvées !

Vous pouvez maintenant fermer la fenêtre **Comodo** : comme votre antivirus, il travaillera à votre protection chaque fois que vous utiliserez votre ordinateur.

En résumé

- Un virus informatique est un programme conçu pour se propager au plus grand nombre de machines possibles. Il peut se dissimuler dans d'autres logiciels, mais aussi dans des mails, fichiers ou pages Internet.
- Un virus peut perturber ou empêcher le fonctionnement d'un ordinateur, ou encore dérober les données qu'il contient.
- Un pare-feu est un logiciel qui surveille toutes les connexions entre un ordinateur et Internet ou tout autre réseau. Il bloque les connexions provenant d'applications malveillantes.

Pour votre protection :

- préférez un compte utilisateur pour votre usage quotidien de l'ordinateur ;
- activez le bloqueur de fenêtres contextuelles de votre navigateur ;
- installez sur votre ordinateur un antivirus gratuit et efficace tel **Avast** ou **AVG** (gratuits) ;
- installez également un pare-feu efficace tel **Comodo** (gratuit) ;
- pour installer **Avast**, **AVG** ou **Comodo**, rendez-vous sur le site Internet de l'éditeur du logiciel concerné. Téléchargez le programme puis suivez les instructions d'installation.

Respectez quelques précautions

Pensez aux mises à jour

Tout utilisateur de l'outil informatique a déjà pu observer ces messages que la machine affiche régulièrement : « *Mises à jour en cours, veuillez ne pas éteindre l'ordinateur* ».

> Que sont ces fameuses mises à jour et surtout, à quoi servent-elles ?

C'est ce que nous verrons ensemble dans la première partie de ce chapitre. Dans la seconde partie, nous ferons le point sur les différents supports de sauvegarde existants, de la solution virtuelle (le *Cloud*) à l'incontournable clé USB ; nous présenterons les avantages et inconvénients de chacun d'entre eux afin de vous aider à faire le meilleur choix.

À quoi servent les mises à jour ?

Il vous est peut-être déjà arrivé, alors que vous êtiez en train de consulter vos mails, de voir s'afficher à l'écran un message de l'ordinateur similaire à : « *Une mise à jour est disponible pour le logiciel ABC. Cliquez ici pour lancer le téléchargement* ». En bas de la fenêtre, un bouton vous permet de reporter l'installation. Il arrive alors fréquemment que l'utilisateur, occupé par une autre tâche, clique sur le bouton ***Reporter***. Bien souvent, il aura même tendance à renouveler ce report, parfois indéfiniment.
Il arrive ainsi que la mise à jour proposée ne soit téléchargée et installée que plusieurs jours après le premier message d'alerte. Dans certains cas, elle ne le sera jamais !

C'est que la plupart d'entre nous ne savent pas exactement à quoi servent ces mises à jour.

> Une application a besoin d'être mise à jour lorsque son éditeur y a apporté des changements. Ces changements peuvent avoir pour objectif d'améliorer le fonctionnement du logiciel (accroître sa vitesse d'exécution, par exemple) ou, bien souvent, de renforcer sa sécurité.

Le piratage informatique peut lui aussi obliger les éditeurs à réaliser de nouvelles mises à jour. En effet, les pirates redoublent sans cesse d'ingéniosité et créent régulièrement de nouveaux virus. **Dès qu'un nouveau virus est découvert, les éditeurs des nombreuses applications existantes effectuent une mise à jour** de leur produit, afin que ce dernier puisse reconnaître ce nouveau virus et s'en

protéger. La mise à jour des applications présentes sur votre ordinateur sont téléchargées par le biais d'internet avant d'être installées.

> Les mises à jour renforcent votre protection ; ne pas les installer peut au contraire vous rendre vulnérable.

Paramétrez vos mises à jour

Heureusement, la majorité d'entre elles, et particulièrement les mises à jour les plus importantes (celles de votre système d'exploitation) sont **automatiques**. Le système a seulement besoin que l'ordinateur soit connecté à Internet. Dès lors, les mises à jour sont envoyées au logiciel et installées sans même que vous en soyez alerté.

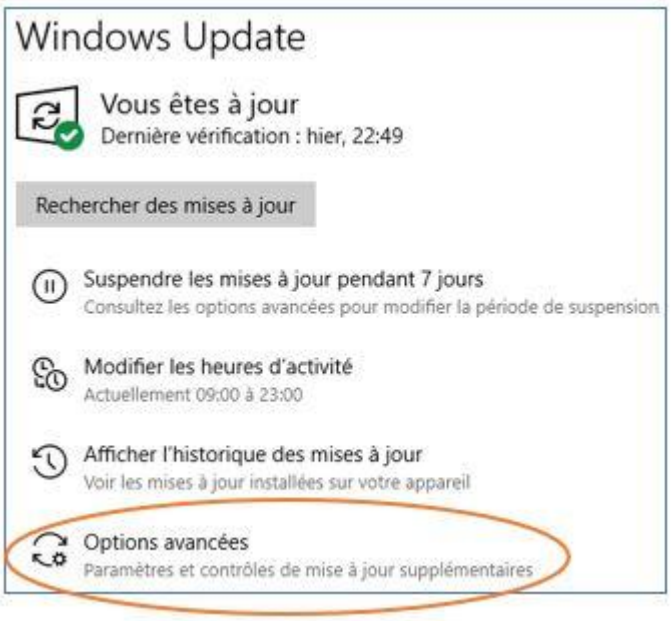
Si votre ordinateur est équipé de **Windows 10**, voici comment le vérifier :

Cliquez sur le bouton Démarrer en bas à gauche de l'écran puis sur la roue crantée représentant les paramètres

Dans la fenêtre Paramètres, cliquez sur Mise à jour et Sécurité

Vous devriez alors voir s'afficher le message « Vous êtes à jour » sous Windows Update (Update : mise à jour, en anglais)

Si vous êtes équipé du Pack Office (Word, Excel, PowerPoint, Outlook, etc.) ou de tout autre logiciel Microsoft, vous pouvez activer leurs mises à jour automatiques :



Cliquez sur Options avancées

Puis activez l'option permettant de « recevoir les mises à jour d'autres produits Microsoft lors de la mise à jour de Windows ».

Si vous utilisez **Internet Explorer, Microsoft Edge ou Mozilla Firefox** comme navigateur Internet, leurs mises à jour se feront alors automatiquement.

Si vous souhaitez connaître le numéro de la version de navigateur installée sur votre ordinateur et savoir si vous disposez bien de la dernière :

- **Avec Firefox :**

1. Cliquez sur le bouton de menu ☰ en haut à droite de l'écran.
2. Cliquez sur **Aide** puis sur **À propos de Firefox**.

(Firefox vérifie alors la présence de mises à jour et les télécharge automatiquement).

- **Avec Google Chrome :**

1. Cliquez en haut à droite de la fenêtre **Google Chrome** sur le bouton **Paramètres**. ⋮
2. Cliquez ensuite sur **Aide** puis sur **À propos de Google Chrome**.

Écran de recherche de mise à jour Google Chrome

Si une mise à jour est disponible, elle s'installera automatiquement.
Dans le cas contraire, cela signifie que vous disposez déjà de la dernière version.
Le numéro de version de **Chrome** est affiché dans la rubrique « **À propos** » (voir image ci-dessus).

Si vous possédez un **Mac**, sachez que le système d'exploitation **macOS** est paramétré pour se mettre à jour automatiquement (cela inclut notamment la mise à jour automatique du navigateur **Safari**).

- Pour le vérifier :

1. Cliquez sur **Préférences Système** dans le menu **Pomme**.
2. Cliquez sur **Mise à jour de logiciels**.
3. Vérifiez que l'option ***« Mettre à jour automatiquement mon Mac »*** est activée.

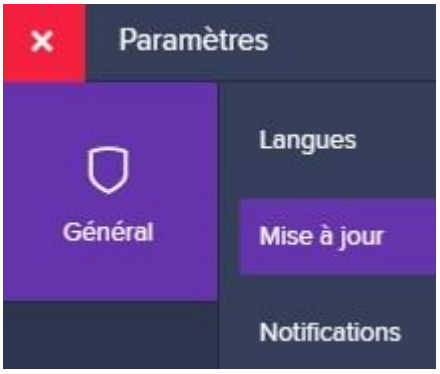
Les antivirus et les pare-feux font également partie des logiciels dont les mises à jour se font automatiquement. Pour le vérifier, il vous suffit de cliquer sur la commande **Mises à jour** de la rubrique **Paramètres**.

- **Exemple avec Avast** :

1. Double-cliquez sur l'icône **Avast** dans la **zone de notification**.

2. Cliquez sur le bouton 

en haut à droite de la fenêtre.



3. Cliquez sur Paramètres puis sur Mises à jour

4. Cliquez sur Plus d'options. 5. Vérifiez que les options "Mise à jour automatique" sont bien activées.

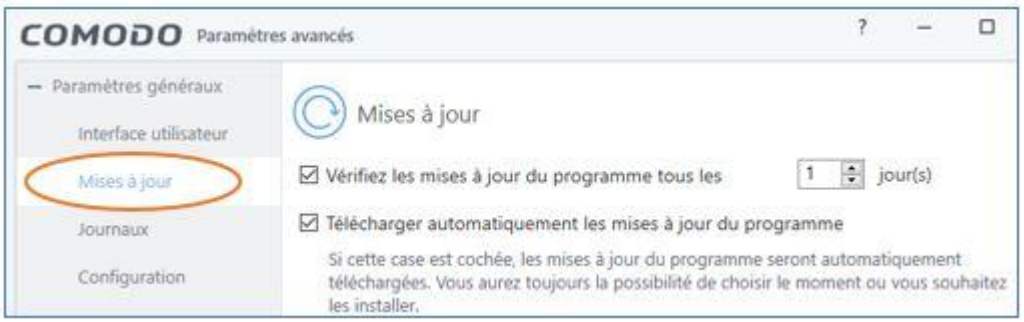
Si vous avez un message indiquant que la base de données virale ou l'application n'est pas à jour, cliquez sur **Rechercher des mises à jour** (**Avast** téléchargera et installera alors la dernière version disponible).

6. Fermez la fenêtre des **Paramètres** puis celle d'**Avast**.

Vérifiez l'option de mise à jour automatique de Comodo :

1. Double-cliquez sur l'icône de **Comodo** dans la zone de notification.

2. Cliquez sur le bouton **Paramètres** en haut de la fenêtre Comodo.



Cliquez sur Mises à jour dans le volet gauche

3. Vérifiez que la case ***Télécharger automatiquement les mises à jour du programme*** est bien cochée.

> En conclusion, pour renforcer votre sécurité, il est en premier lieu important de vérifier que votre système d'exploitation soit paramétré pour effectuer automatiquement les mises à jour.

> De même pour vos logiciels antivirus et pare-feu, ainsi que pour votre navigateur Internet.

Enfin, même si vous pouvez sans problème reporter une mise à jour qui vous est proposée parce que vous êtes alors occupé à une autre tâche, d'une manière générale il est **recommandé de toujours accepter l'installation des mises à jour**.

> En informatique comme en médecine, le risque zéro n'existe malheureusement pas.

Certes, si vous respectez les règles présentées dans ce cours, il y a peu de chances que vous soyez un jour victime d'un virus ou d'une attaque malveillante. Ce qui ne doit pas vous empêcher de prendre toutes les précautions nécessaires : en cas d'attaque malveillante, vos données courent en effet le risque d'être endommagées. Or, la perte de vos données ne sera pas un problème si… vous avez pensé à réaliser une copie de sauvegarde.

Sauvegardez vos données

Utilité des sauvegardes

Nous possédons tous de nombreux fichiers, soit à titre personnel, soit liés à notre activité professionnelle. Nos données privées (vidéos ou photos de famille ou d'amis, par exemple) ont souvent bien plus d'importance à nos yeux que de « simples » données informatiques : elles contiennent nos **souvenirs**, et sont, à ce titre, **inestimables** et… **irremplaçables**.

Le **stockage des données privées** est ainsi devenu une **préoccupation** grandissante pour bon nombre d'entre nous. D'autant plus que depuis quelques années, notre société nous encourage à la dématérialisation, notamment pour les démarches administratives, par exemple.

> Si ces nouvelles façons de procéder ont l'avantage de diminuer notre consommation de papier, elles génèrent en retour un nouveau problème : celui du stockage des données.

Ces dernières sont certes stockées sur le disque dur de votre ordinateur, mais il est prudent et fort recommandé d'effectuer au minimum une **double sauvegarde** : une copie de vos données qui sera enregistrée sur un autre support. Votre ordinateur n'est en effet **pas à l'abri d'un vol**, d'une **panne** ou d'un **accident** quelconque, qui le rendrait inutilisable et entraînerait la perte de tous les fichiers qu'il contient.

Il existe plusieurs moyens de sauvegarder vos données ; chacun ayant bien entendu ses avantages et ses inconvénients. Nous allons donc passer ensemble en revue les grands types de supports de stockage que l'on peut trouver actuellement.

Les différents supports de sauvegarde

> Vaut-il mieux un stockage virtuel ou matériel ?

Le Cloud

Pour le stockage virtuel, on fait référence au stockage en ligne, au moyen du ***Cloud***.

> Lorsque des données sont stockées dans le **Cloud**, elles sont en réalité enregistrées, via Internet, sur des serveurs (sorte d'ordinateurs très puissants) enfermés dans des centres de données (en anglais, *data centers*).

> Ces centres sont situés dans des bâtiments très résistants et sécurisés. À tel point que leur emplacement géographique est souvent tenu secret. Concrètement, ils contiennent des centaines de serveurs, ressemblant à de grosses armoires et remplis de disques durs.

Les transferts de fichiers entre le Cloud et votre ordinateur se font de manière **sécurisée** : la transmission est systématiquement **chiffrée**, et vous seul êtes en mesure d'accéder à vos données. Pour cela, comme pour tout autre compte en ligne, vous disposez d'un **identifiant** et d'un **mot de passe**, souvent doublés d'un service de **double authentification.**

Par rapport au stockage matériel, le stockage en ligne présente certains **avantages**, dont celui de permettre l'**accès à vos fichiers à partir de n'importe quel ordinateur et quel que soit l'endroit** où vous vous trouvez.

La majorité de ces services incluent également une **option de synchronisation :**

Imaginez que vous sauvegardiez dans le Cloud l'intégralité de votre disque dur.

Quelques jours plus tard, ayant **importé de nouvelles photos** dans le dossier *Images* de votre ordinateur, vous souhaitez les ajouter également à vos données dans le Cloud. Vous n'avez ni l'envie ni le besoin de copier de nouveau la totalité de vos fichiers, ce serait une perte de temps.

Si le service que vous utilisez propose la synchronisation et que vous avez activé cette option dans les paramètres de votre compte, il sera alors **capable de détecter automatiquement** l'ajout de nouvelles images et de les sauvegarder, sans aucune intervention de votre part.

Enfin, le stockage en ligne permet de **repousser les limites inhérentes au stockage physique** : les ordinateurs actuellement sur le marché possèdent des disques durs dont la capacité peut varier de **500 Go à 4 To**, tandis que le Cloud ne vous imposera aucune limite. Il permet un espace de **stockage illimité** pour ceux qui sont disposés à en payer le **prix** !

Car s'il est vrai que les principaux fournisseurs de ce service proposent tous un espace de **stockage gratuit**, celui-ci est la plupart du temps relativement **faible**. Ce qui constitue d'ailleurs le **principal inconvénient** de ce type de stockage.

Pour indication, vous trouverez dans le tableau ci-dessous quelques-uns de ces services parmi les plus connus, avec la quantité d'espace de stockage offerte gratuitement :

Fournisseur	**Espace de stockage gratuit**

Mega	20 Go
Google Drive	15 Go
pCloud	10 Go
OneDrive (Microsoft)	5 Go
Apple iCloud	5 Go
Dropbox	2 Go

Prêtez également attention à la qualité de votre connexion Internet : pour fonctionner correctement, le stockage des données dans le Cloud nécessite en effet une **connexion de bonne qualité**.

Le NAS

Pour contrer les limites du Cloud, un nouveau type de stockage a émergé ces dernières années : il s'agit du **NAS** ou ***Network Attached Storage*** :

Issu du monde de l'entreprise, Le **NAS** ou **unité de stockage en réseau**, commence à apparaître dans les foyers français ; on peut le comparer à une sorte de Cloud personnel ou Cloud domestique.


Exemple de NAS personel

Équipé d'un ou plusieurs disques durs (en fonction du modèle choisi), il permet de stocker dans un même endroit l'ensemble des données provenant de tous les appareils d'un foyer (téléphones, tablettes, consoles de jeux et ordinateurs) qui peuvent d'ailleurs y accéder simultanément.

Pour pouvoir l'utiliser, votre domicile doit disposer d'un **réseau local** auquel seront connectés l'ensemble de vos appareils. Ce qui est le cas de la plupart des foyers, puisqu'il suffit pour cela d'être équipé d'une **box Internet**.
L'**installation** est en outre **extrêmement simple** puisqu'elle se résume à relier le serveur NAS à votre box au moyen d'un câble Ethernet.

Le NAS apparaîtra alors sous la forme d'un dossier dans l'explorateur de fichiers de votre ordinateur. Pour y stocker vos données, il suffira de les copier/coller de votre ordinateur vers le dossier NAS apparent.

Vos données y seront enregistrées de manière sécurisée (les fichiers seront chiffrés).

Comparé au Cloud qui impose de payer chaque mois un abonnement à tous ceux qui possèdent de grandes quantités de données, cette solution offre **l'avantage d'augmenter considérablement la quantité d'espace de stockage disponible pour vos fichiers**.

Sachez également qu'un NAS consomme beaucoup moins d'électricité qu'un ordinateur branché sur le secteur.

Son principal **inconvénient** reste toutefois son **prix d'achat** : si vous souhaitez disposer chez vous de votre Cloud personnel, il vous en coûtera en moyenne de 180 € (pour 2 To de stockage) à 500 € (8 To).

Si vous n'êtes tenté ni par le Cloud, ni par le NAS, rien n'est perdu !

Le disque dur et la clé USB

Ainsi, une personne qui possède à la fois un ordinateur fixe et un ordinateur portable peut tout à fait effectuer une double sauvegarde de ses données sur les 2 ordinateurs à la fois. Si par malheur l'un des deux devenait inutilisable, les données ne seront pas perdues puisque qu'elles seront toujours accessibles sur le second disque dur interne à l'ordinateur.

Que vous possédiez un ou plusieurs ordinateurs, vous pouvez également opter pour une sauvegarde sur **disque dur externe**.

De taille relativement petite (2,5 pouces en moyenne), le disque dur externe ressemble à un rectangle de métal et ne prend pas plus de place qu'un livre de poche. Il est en outre très facile à utiliser, puisqu'il suffit pour cela de le brancher à ordinateur via un câble USB.

Comme dans le cas d'un NAS, il apparaîtra sous la forme d'un dossier dans l'explorateur de fichiers de votre ordinateur.

Mais la solution la plus simple et la moins onéreuse financièrement reste la sauvegarde sur **clé USB**. Idéale pour les **petits budgets**, elle est extrêmement pratique car petite, amovible et **facilement transportable**.

Les prix d'un disque dur externe comme d'une clé USB varient en fonction de leur capacité de stockage et de la vitesse de transfert proposée (correspond au temps nécessaire pour copier des données de votre ordinateur vers la clé et vice-versa).

Le tableau ci-dessous vous indique les prix moyens proposés dans le commerce en fonction de la mémoire disponible :

Clé USB	
Prix dé départ	**Espace de stockage**
6 €	8 Go
10 à 15 €	16 Go
15 à 20 €	32 Go

110 à 130 €	256 Go
250 à 300 €	512 Go
500 €	1 To (= 1.000 Go)

Disque dur externe

Prix de départ	**Espace de stockage**
25 €	160 Go
30 €	250 Go
50 €	500 Go
50 à 100 €	1 To
60 à 100 €	2 To
120 à 200 €	4 To
340 €	10 To

Attention toutefois à la petite taille d'une clé USB, car si elle présente un avantage évident, elle constitue aussi son principal **inconvénient** : comme tous les petits objets, il est en effet facile (trop facile) de **l'égarer** !

Beaucoup optent d'ailleurs pour l'achat de 2 clés USB, chacune contenant les mêmes fichiers.

Le **premier critère de choix** d'un support est bien souvent relatif au **budget** que l'on veut y consacrer. Il faut ensuite déterminer si vous vous **déplacez** souvent et si vous avez besoin d'accéder à vos données durant vos déplacements.

Dans ce cas, le Cloud sera le mieux placé pour ceux qui sont prêts à payer un abonnement, tandis que la **clé USB ou le disque dur externe** seront une meilleure solution pour les **petits budgets** ou pour tous ceux qui ne souhaitent **pas stocker virtuellement leurs données**.

Enfin, si vous êtes davantage sédentaire et que vous avez de **grosses quantités de données** à stocker, vous pourrez opter pour le serveur **NAS**.

À vous maintenant de choisir le support le plus adapté à votre cas ! 

En résumé

- Les mises à jour ont pour but d'améliorer vos applications. Elles sont importantes pour la sécurité de votre ordinateur et la protection de vos données.
- Il est recommandé de vérifier que votre système d'exploitation est paramétré pour effectuer automatiquement les mises à jour. Cette vérification doit également être effectuée pour les applications suivantes : navigateur Internet, antivirus et pare-feu.
- Lorsque votre ordinateur vous avertit qu'une mise à jour est disponible pour l'un de vos logiciels, procédez sans trop tarder à son installation.
- Sauvegarder vos données est une précaution essentielle qui vous protège contre toute détérioration ou perte de vos fichiers, quelle qu'en soit la cause.
  Il existe pour cela plusieurs solutions :
  - le stockage de données dans le Cloud a l'avantage de rendre ces dernières accessibles de n'importe quel endroit et d'offrir un espace de stockage illimité, à condition d'être prêt à payer un abonnement. Il offre toutefois un stockage gratuit si vous ne dépassez pas 50 Go de données ;
  - le NAS est un serveur (ordinateur super puissant) destiné à un usage privé comme professionnel. Il se connecte au réseau de votre box Internet et permet de stocker l'ensemble des données de tous les appareils du foyer. Son prix varie de 180 à 500 €, en fonction de la quantité d'espace de stockage disponible ;
  - le disque dur externe se branche sur le port USB de votre ordinateur. De petite taille et simple à utiliser, son prix varie de 25 à plus de 300 €, pour un stockage allant de 160 Go à 4 To.
  - adaptée aux petits budgets, simple et pratique, la clé USB permet le stockage de 8 Go à 1 To de données ; une solution pratique et économique. Attention toutefois à ne pas l'égarer !

Ce support de cours est librement inspiré du cours de ***Claire Castello,*** ***"Découvrez les bases de la sécurité numérique" sur OpenClassRooms*****.**