Parcours : DISCOVERY

Module : Naviguer en toute sécurité

Projet 1 - Un peu plus de sécurité, on n'en a jamais assez !

Sommaire

1 - Introduction à la sécurité sur Internet

Réponse 1

Article 1 = ANSSI - Dix règles de base

● Article 2 = Economie.gouv - Comment assurer votre sécurité numérique

● Article 3 = Site W - Naviguez en toute sécurité sur Internet

● Article bonus = wikiHow - Comment surfez en sécurité sur internet

2 - Créer des mots de passe forts

C'est fait

3 - Fonctionnalité de sécurité de votre navigateur

Réponse 1

Les sites web qui semblent être malveillants sont :

● www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l'univers Marvel

● www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde

● www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé

Les seuls sites qui semblaient être cohérents sont donc :

● www.dccomics.com, le site officiel de l'univers DC Comics

● www.ironman.com, le site officiel d'une compétition internationale de triathlon (et non du super-héros issu de l'univers Marvel)

Réponse 2

C'est ok, les paramètres par défaut de ces deux navigateurs sont réglés pour réaliser les mises à jour automatiquement. Comme d'habitude, Firefox affiche une personnalisation des paramètres un peu plus poussée.

4 - Éviter le spam et le phishing

Réponse 1

Jigsaw | Quiz sur l'hameçonnage (phishingquiz.withgoogle.com)

5 - Comment éviter les logiciels malveillants

Réponse 1

● Site n°1

○ Indicateur de sécurité

■ HTTPS

○ Analyse Google

■ Aucun contenu suspect

● Site n°2

○ Indicateur de sécurité

■ Not secure

○ Analyse Google

■ Aucun contenu suspect

● Site n°3

○ Indicateur de sécurité

■ Not secure

○ Analyse Google

■ Vérifier un URL en particulier (analyse trop générale)

TESTE : Why No HTTPS? The World's Largest Websites Not Redirecting Insecure Requests to HTTPS

6 - Achats en ligne sécurisés

Réponse 1 : c'est fait

Voici un exemple d'organisation de libellé pour gérer la messagerie électronique :

● Achats : historique, facture, conversations liés aux achats

● Administratif : toutes les démarches administratives

● Banque : tous les documents et les conversations liés à la banque personnelle

● Création de compte : tous les messages liés à la création d'un compte (message de bienvenue, résumé du profil, etc.

● Job : tous les messages liés à mon projet professionnel

● SAYNA : tous les messages liés mon activité avec SAYNA

7 - Comprendre le suivi du navigateur

C’est fait : Objectif : exercice présent sur la gestion des cookies et l’utilisation de la navigation privée

Les cookies tiers ne sont pas forcément nécessaires pour profiter des ressources disponibles sur Internet : pour limiter vos traces, il est recommandé de les refuser par défaut.

Pour limiter vos traces, vous pouvez effectuer deux actions :

- **limiter** l'utilisation des cookies, dans les paramètres de votre navigateur (sur votre ordinateur ou sur votre téléphone) ou en utilisant la navigation privée ;
- **effacer** les cookies déposés par les sites web sur votre appareil.

Vous retrouverez souvent les mêmes termes (« interdire les cookies », « effacer les données de navigation »), mais la marche à suivre sera souvent différente d'un navigateur à l'autre.

Les paramétrages présentés dans cette page visent à empêcher les tiers de pouvoir suivre votre navigation.

Firefox

Sur ordinateur

Paramétrer la gestion des cookies et traceurs

1. En haut à droite de la fenêtre de votre navigateur, sélectionnez **le menu ☰**, puis **paramètres**
2. Dans la page qui vient de s'ouvrir, cliquez sur l'onglet **Vie privée et sécurité**
3. Dans le menu **Protection renforcée contre le pistage** qui apparaît, sélectionnez la protection qui répond à vos besoins :

- la **protection standard** est recommandée pour limiter vos traces dans un usage normal : elle permet de bloquer la plupart des traqueurs, cookies en navigation normale et en navigation privée ;
- la **protection stricte** bloque davantage de mécanismes de pistage, mais peut empêcher le navigateur de fonctionner correctement (par exemple pour le chargement de vidéos ou lors de certaines actions sur une page) ;
- la **protection personnalisée** vous permet de régler les différentes options proposées par le navigateur.
- vous pouvez également activer l'option **Envoyer aux sites web un signal « Ne pas me pister » indiquant que vous ne souhaitez pas être pisté·e** en cliquant sur le bouton **Toujours**.

5. Dans la partie **Cookies et données de sites**, vous pouvez notamment :

- effacer les cookies présents dans votre navigateur ;
- effacer automatiquement tous les cookies présents dans le navigateur quand vous le fermerez.

Supprimer les données de navigation

Dans le menu, sélectionnez **Bibliothèque**, puis **Historique**, et enfin **Effacer l'historique récent**.
Vous pouvez également réaliser cette manipulation en appuyant simultanément sur les touches **Ctrl** + **Maj** + **Suppr** de votre clavier.

Sur téléphone et tablette

Firefox mobile

L'application Firefox pour téléphone est similaire à la version pour ordinateur. Elle offre quelques options pour protéger votre privée.
Dans le menu en bas à droite de votre application, sélectionnez **Paramètres** puis descendez dans la partie **Vie privée et sécurité**.
Vous pouvez gérer les paramètres suivants :

- **« Protection renforcée contre le pistage »**, qui permet de choisir une protection qui s'applique en navigation normale ou en navigation privée ;
- **« Cookies »**, qui permet de refuser certains types de cookies, comme les cookies tiers, c'est-à-dire ceux déposés par d'autres sites (publicités, lecteurs de vidéos, etc.), ou encore les cookies utilisés pour le pistage (publicité, etc.) ;

- vous pouvez également **demander à l'application d'effacer vos traces (dont les cookies) en fermant l'application**.
  Supprimer vos traces

1. Dans le **menu ⋮** en bas à droite de votre application, sélectionnez **Paramètres ;**
2. Dans la partie **Vie privée**, sélectionnez **Supprimer les données de navigation**. Vous pouvez également supprimer certains types de données (par exemple les cookies).

Firefox Focus

L'application Firefox Focus est similaire à l'application Firefox pour mobile, mais propose davantage d'options pour contrôler votre vie privée.
Dans le menu en haut à droite de votre application, sélectionnez **Paramètres** puis **Vie privée et sécurité**. Vous pouvez alors gérer en détail les options concernant votre vie privée :

- les traqueurs publicitaires ;
- les traqueurs de statistiques ;
- les traqueurs de réseaux sociaux ;
- les autres traqueurs de contenus ;
- vous pouvez également interdire certains types de cookies (rubrique **Cookies et données de sites**).

Supprimer vos traces

L'application Firefox Focus supprime automatiquement les contenus enregistrés sur l'appareil (historique, cookies, etc.) lorsque vous fermez l'application.

Chrome

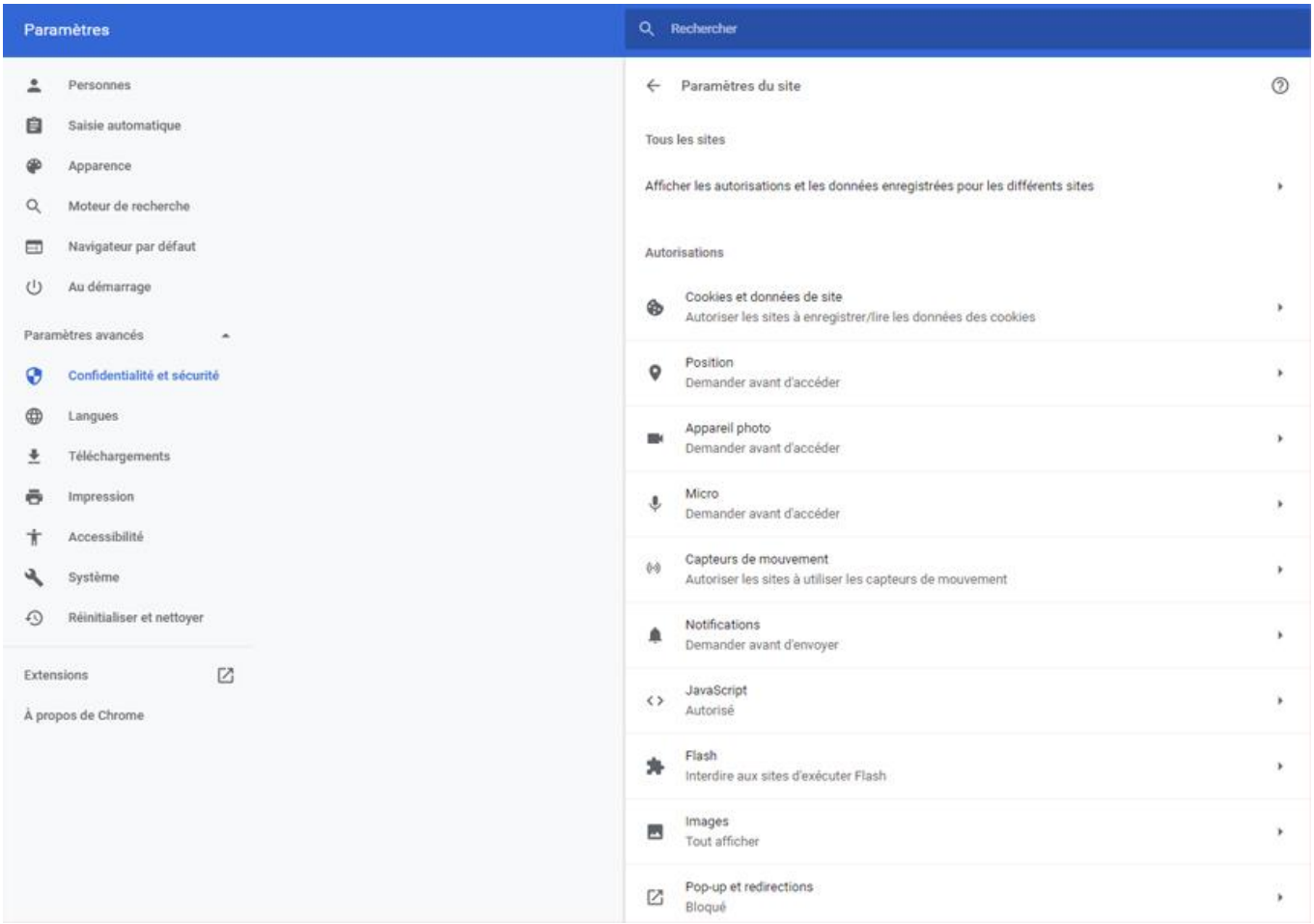
Sur ordinateur

Paramétrer la gestion des cookies et traceurs

1. Cliquez sur l'icône de **menu ⋮** en haut, à droite de la barre d'adresse ;
2. Sélectionnez **Paramètres** ;
3. Sélectionnez **Sécurité et confidentialité** :

- Dans cette page, vous pouvez sélectionner **Envoyer une demande « Interdire le suivi » pendant la navigation**.

5. Sélectionnez **Paramètres du site** dans la partie principale de la page **;**
6. Sélectionnez **Cookies et données de sites** dans la partie principale de la page.



Chrome propose quelques options sur cette page, notamment :

- **bloquer les cookies tiers**, c'est-à-dire ceux déposés par d'autres sites que celui que vous visitez ;
- **effacer les cookies et les données de site en quittant Chrome**.

Effacer les données de navigation

Cliquez sur l'icône de menu en haut, à droite de la barre d'adresse, sélectionnez **Historique**, puis **Effacer les données de navigation** dans le menu de gauche.
Vous pouvez également réaliser cette manoeuvre en appuyant simultanément sur les touches **Ctrl** + **Maj** + **Suppr** de votre clavier.

Sur téléphone et tablette (version 79)

En haut à droite de l'application, sélectionnez le menu (matérialisé par trois points) puis **Paramètres** (en bas) puis **Confidentialité** (dans paramètres avancés).
Sur cette page, vous pouvez sélectionner :

- **interdire le suivi**, qui demande aux sites que vous visitez de ne pas vous suivre ;
- **effacer les données de navigation** (historique, cookies, images, etc.).

8 - Principes de base de la confidentialité des médias sociaux

10 conseils pour être en sécurité sur les médias sociaux

Découvrez comment protéger simplement et efficacement sa vie privée en ligne.

Parallèlement à cela, les réseaux sociaux tentent tant bien que mal à jouer le jeu de la sécurité. Mais des efforts sont faits notamment du côté de Facebook, avec des paramètres de confidentialité améliorés.
Il y a aussi des réseaux sociaux qui ont le vent en poupe, ce sont ceux qui sont **anonymes** ou ceux ayant des publications qui « ***disparaissent*** » après un certain temps.

Mais est-ce vraiment suffisant ? Au lieu d'attendre que les plateformes en ligne renforcent leur sécurité, il vaut mieux que de nous-même, nous agissions dès maintenant en étant plus vigilant.

Les conseils

Voici donc les 10 conseils que **YOURinfoGRAPHIC** nous propose d'appliquer pour être en sécurité sur les médias sociaux :

1.Créer son anonymat
Créez une nouvelle adresse email. Ne pas avoir de caractéristiques identifiables (telles que nom et prénom, année de naissance, ou un code postal) dans l'adresse e-mail ou les paramètres de profil. Créez des pages sur les réseaux sociaux en utilisant cette nouvelle adresse e-mail et ajouter seulement ceux en qui vous avez vraiment confiance. Évitez également l'identification des photos.

2. Utiliser des mots de passe forts
Mettez à jour vos mots de passe pour tous les comptes que vous avez, et assurez-vous d'utiliser des mots de passe forts sur tous les nouveaux comptes que vous créez. Utilisez des lettres (au moins une MAJUSCULE) et des chiffres, et envisagez également d'utiliser des caractères spéciaux (! @ # $ %). Ne pas utiliser un mot de passe que l'on peut deviner.

3. Augmenter et améliorer ses paramètres de confidentialité
Chaque réseau social possède une option pour « les paramètres de confidentialité » pour vous permettre d'augmenter la sécurité de votre compte, de sorte à ce que seuls vos amis ou des listes spécifiques de personnes peuvent voir vos messages et informations privées. Ne laissez jamais les paramètres par défaut.

4. Éviter de se faire identifier par la localisation
Désactivez les paramètres de localisation et ne partagez jamais l'endroit où vous serez (y compris les sorties en ville et en vacances). De même, ne partagez pas l'information après coup, les gens peuvent noter vos habitudes et prédire quand et où vous allez être.

5. Ajouter des amis attentivement
Soyez sûr que vous connaissez les personnes qui vous ajoutent. Envoyez un message privé avant d'accepter une demande d'ami et demandez à la personne quelque chose qui prouve qui elle est. Même si vous pensez avoir reconnu le nom ou la photo, on n'est jamais trop prudent (c'est une technique de piratage répandue).

6. Ne pas partager des informations personnelles
Cela comprend les numéros d'assurance sociale, adresse, nom de jeune fille de votre mère, l'année de naissance, numéro de téléphone et coordonnées bancaires. Ceux-ci peuvent être utilisés par des voleurs d'identité. Si quelqu'un a légitimement besoin de ces informations, ils peuvent vous contacter d'une autre façon.

7. Publier, republier, aimer
Rien sur Internet n'est complètement sûr. N'importe qui peut enregistrer ou faire une capture d'écran ce que vous publiez et partagez, alors faites attention à vos publications. Supposons que tout ce que vous postez est permanent. Ne publiez jamais rien sur vous, votre famille, vos amis que vous (et eux) ne voulez que cela soit public. Ne jamais poster quelque chose que vous pourriez regretter.

8. Protéger son image et sa réputation
Si quelqu'un publie quelque chose sur vous que vous n'aimez pas, dites que cela vous rend mal à l'aise et demandez à retirer le contenu. Vérifiez périodiquement « photos de moi » pour voir si quelqu'un a posté, et vérifiez votre mur pour voir si vous êtes « tagué ». Si quelqu'un refuse de retirer quelque chose sur vous, vous pouvez bloquer la personne et/ou la signaler.

9. Faire attention aux liens frauduleux
Les pirates peuvent casser votre compte ou un virus peut se propager si vous cliquez sur les liens dont vous n'êtes pas sûr. Si quelqu'un publie quelque chose qui vous ne pensez pas qu'il le ferait en temps normal, ou quelque chose qui vous semble étrange, envoyez-leur un message à ce sujet et faites-leur savoir que vous pensez qu'ils ont peut-être été piraté.

10. Connaître les mesures à prendre
Si vous êtes victime de harcèlement, veuillez sauvegarder (ou faire une capture d'écran) la communication ou la publication offensive. Signalez-les sur le site et contactez les personnes qui peuvent vous aider dans cette situation (comme un avocat, un conseiller ou un travailleur social).

9 - Que faire si votre ordinateur est infecté par un virus

1. **Si vous pensez être infecté par un virus** : ne réalisez plus aucune opération sensible sur votre appareil comme, par exemple, consulter votre compte bancaire, envoyer des informations confidentielles ou vous connecter sur un service en ligne qui nécessite que vous renseigniez un nom d'utilisateur et un mot de passe.

2. **Déconnectez l'équipement infecté d'Internet ou du réseau** pour éviter que le virus ne se propage à d'autres appareils. Pour cela, débranchez le câble réseau (Ethernet) de votre ordinateur ou de votre serveur ou désactivez la connexion Wi-Fi et/ou Bluetooth de votre appareil ou les connexions de données s'il s'agit d'un appareil

mobile (téléphone, tablette).

3. **Identifiez la source de l'infection** (faille de sécurité, message malveillant) et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire. L'infection peut par exemple provenir de l'ouverture d'une pièce jointe, d'un clic sur un lien malveillant contenu dans un message (mail, MMS) ou bien encore en naviguant sur un site malveillant. Il peut également s'agir d'une intrusion due à un logiciel ou un appareil non mis à jour ou mal configurés (port serveur non fermé ou peu sécurisé…), etc. Enfin, il peut s'agir aussi d'applications qui ont été téléchargées et qui pourraient contenir un virus (logiciels ou jeux piratés, applications mobiles peu fiables…).

4. **Évaluez l'impact et l'étendue de l'infection.** Vérifiez que le virus ne s'est pas propagé à d'autres appareils ou équipements de votre réseau informatique. Mesurez les conséquences de l'infection et identifiez les éventuelles informations perdues ou compromises.

5. **Récupérez ou tentez de faire récupérer par un professionnel les preuves disponibles**. Séquestrez la ou les machines touchées ou réalisez-en une copie physique complète. Ces éléments peuvent permettre d'obtenir des « traces » du cybercriminel dans le cadre de l'analyse de l'attaque. Ils peuvent également constituer des preuves à valeur juridique en cas de procédures ultérieures.

6. Avant de remettre en état votre système, et en fonction du préjudice subi, **déposez plainte** au commissariat de police ou à la brigade de gendarmerie ou en adressant votre plainte au procureur de la République du tribunal judiciaire dont vous dépendez. Tenez à disposition tous les éléments de preuves techniques en votre possession. Il est important de garder à l'esprit que le dépôt de plainte doit intervenir avant la réinstallation des appareils touchés afin de conserver les preuves techniques de l'incident et pouvoir les fournir aux enquêteurs.

7. Après avoir vérifié que votre antivirus est en état de fonctionnement et à jour, **faites une analyse antivirale complète (scan) de vos appareils**. Si votre antivirus détecte des logiciels malveillants, il vous proposera de les « mettre en quarantaine », c'est-à-dire de les empêcher d'agir, ou, mieux, de les supprimer directement lorsque cela est possible. Redémarrez votre appareil après cette opération.

8. **Changez au plus vite vos mots de passe** au moindre doute sur leur piratage. Utilisez des mots de passe différents et complexes pour chaque site et application utilisés.

9. **Restaurez votre système** si les symptômes de l'infection continuent de se manifester. En effet, les systèmes d'exploitation actuels intègrent des fonctionnalités qui permettent de restaurer le système de votre ordinateur à une date antérieure, ce qui permettra d'annuler les modifications qui ont été apportées à votre appareil sans affecter vos fichiers personnels. Référez-vous à la documentation de votre appareil pour en savoir plus, ou effectuez une recherche sur Internet.

10. **Réinitialisez ou réinstallez complètement votre appareil en dernier recours** si le virus persiste toujours. Cette action permettra de le remettre dans ses paramètres d'usine. N'oubliez pas d'effectuer une sauvegarde de vos fichiers personnels avant cette opération car vous perdrez les données stockées sur l'appareil (tous nos conseils pour gérer au mieux vos sauvegardes).

11. **Faites-vous assister au besoin par des professionnels qualifiés**. Vous trouverez sur www.cybermalveillance.gouv.fr des professionnels en cybersécurité susceptibles de vous apporter leur assistance technique.

Un exercice pour installer et utiliser une antivirus + antimalware en fonction de l'appareil utilisé

1. Qu'est-ce qu'un virus ?

C'est un petit programme encombrant qui a été incorporé à un contenu hôte (autre programme, données **téléchargées**, **mails**, etc) et qui a la particularité de se propager à l'intérieur de votre ordinateur et via votre connexion **Internet**.

Il peut avoir plusieurs fonctions comme récolter vos données personnelles et de consultation ou utiliser les composants et la connexion de votre ordinateur, ralentissant son usage et par la même votre connexion. Très souvent inoffensifs, on peut les considérer comme de petits parasites encombrants qu'il faut régulièrement nettoyer.

Les plus agressifs d'entre eux peuvent cependant endommager les données de votre ordinateur (ces virus sont appelés **Malware** ou **Maliciel**) ou prendre votre appareil en otage en échange d'une rançon et sans certitude de retrouver vos données (on les appelle **Ransomware**, « **logiciel** rançon » en anglais). Ces virus se neutralisent grâce à un **antimalware** mais peuvent parfois nécessiter d'effacer complètement le **disque dur** de l'ordinateur pour s'en débarrasser totalement.

2. Que fait un antivirus ?

Le rôle d'un antivirus est de scanner le contenu de votre ordinateur ainsi que votre connexion Internet afin de localiser et neutraliser d'éventuels virus. Une fois le virus supprimé, ces logiciels sont capables de reconstituer la partie de l'ordinateur qui a été modifiée par le virus.

3. Où télécharger un antivirus ?

De nombreux sites de téléchargements de logiciels vous offrent la possibilité de **télécharger** vos antivirus en toute sécurité. Parmi ces sites, on retrouve : 01Net.com, Commentçamarche.com ou encore Clubic. Leur contenus sont vérifiés et sécurisés. Vous avez donc peu de chances de tomber sur un logiciel malveillant. Sélectionnez votre **système d'exploitation** ou tapez le nom du logiciel que vous cherchez et laissez vous guider dans votre téléchargement.

4. Quel antivirus télécharger ?

C'est LA grande question que tout novice (et même moins novice) se pose lorsqu'il s'agit de protéger son ordinateur et ses contenus des attaques de virus. Il y a tout d'abord plusieurs choses à savoir :

4.1 Un antivirus pour quel système d'exploitation ?

- Le **système d'exploitation Windows** est le plus touché par les virus. Il est le plus populaire et a peu de versions différentes, ce qui laisse l'opportunité aux créateurs de virus de chercher les plus petites failles du système afin de propager plus facilement leurs logiciels désagréables.
- Les ordinateurs sous MacOS (le **système d'exploitation Apple**) rencontrent moins ce problème car la firme bride davantage le contenu de ses programmes et fait en sorte de bloquer les accès les plus vulnérables. Ce qui a pour avantage de protéger les ordinateurs Apple mais qui rend plus difficile le changement d'éléments séparés de l'ordinateur (et qui revient donc plus cher).
- Quant à **Linux**, il est quasiment invulnérable de par la constitution même de son système : c'est un noyau autour duquel sont rajoutés les éléments nécessaires à des tâches et fonctionnements particuliers. Il existe des milliers de versions et sous-versions de Linux, ce qui rendrait rapidement inefficace toute propagation de virus dont l'existence même repose sur les failles systématiques de leur hôte.

Attention
Bien que les ordinateurs sous MacOs soient moins vulnérables aux virus, il est toutefois recommandé de les protéger également avec un antivirus (et un antimalware). En effet, même s'ils sont moins touchés, ils peuvent être impactés et transmettre les virus (par voie de mail par exemple) à d'autres ordinateurs sous Windows.

4.2 La diversité d'application des antivirus

Il n'existe actuellement pas d'antivirus parfait supprimant tous les antivirus et autres malwares du **web**. La pertinence de votre antivirus dépendra avant tout de l'utilisation que vous avez de votre ordinateur. Si vous êtes un utilisateur averti qui fait relativement attention à la consultation de ses **mails** et ses **téléchargements**, votre besoin de protection ne sera pas nécessairement porté sur les mêmes failles que peut rencontrer un utilisateur non averti.

Pour mieux comprendre les différences d'application des antivirus, je vous invite à lire cet article, qui est fréquemment mis à jour et qui peut vous aider à faire votre choix.

Vous trouverez également ici un article de Clubic vous présentant une sélection d'antivirus selon leurs principaux rayons d'action et leurs divers offres, gratuites ou payantes.

Conseil
Il n'est pas obligatoire de payer votre antivirus pour qu'il protège votre ordinateur. Beaucoup de fournisseurs d'antivirus proposent des services gratuits (bien qu'ayant de la publicité) permettant de sécuriser correctement votre appareil et vos données. Vous avez cependant le choix de payer pour obtenir les services complémentaires proposés par le fournisseur.

5. Télécharger un antivirus

L'un des antivirus les plus téléchargés est **Avast Antivirus**. Comme la plupart des antivirus, vous avez le choix entre une version payante ou une version gratuite du logiciel. La version gratuite est amplement suffisante pour protéger votre ordinateur des virus. La version payante vous propose une interface sans publicités et des outils complémentaires à la version gratuite.

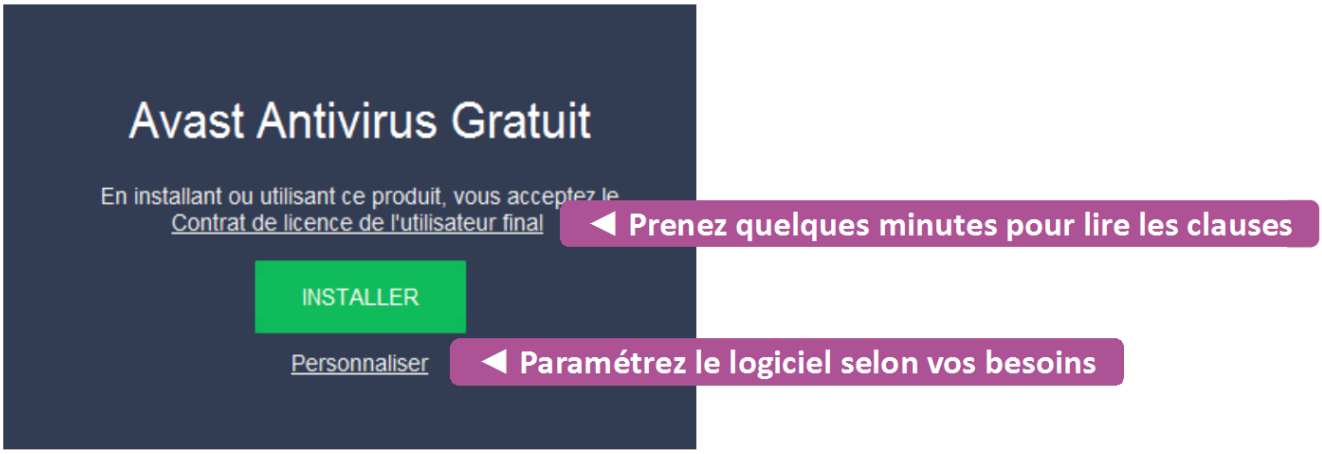
Télécharger Avast Antivirus

Attention
Par défaut, le téléchargement proposé est celui du système d'exploitation Windows, mais si vous disposez d'un appareil Apple, vous devrez choisir la compatibilité Mac et s'il s'agit de votre mobile, utilisez la version pour Android.

Partenariat oblige, lorsque vous cliquez sur le bouton de téléchargement, vous êtes redirigé vers le site 01.net qui vous permet de télécharger en toute sécurité une grande partie des logiciels actuellement sur le marché.

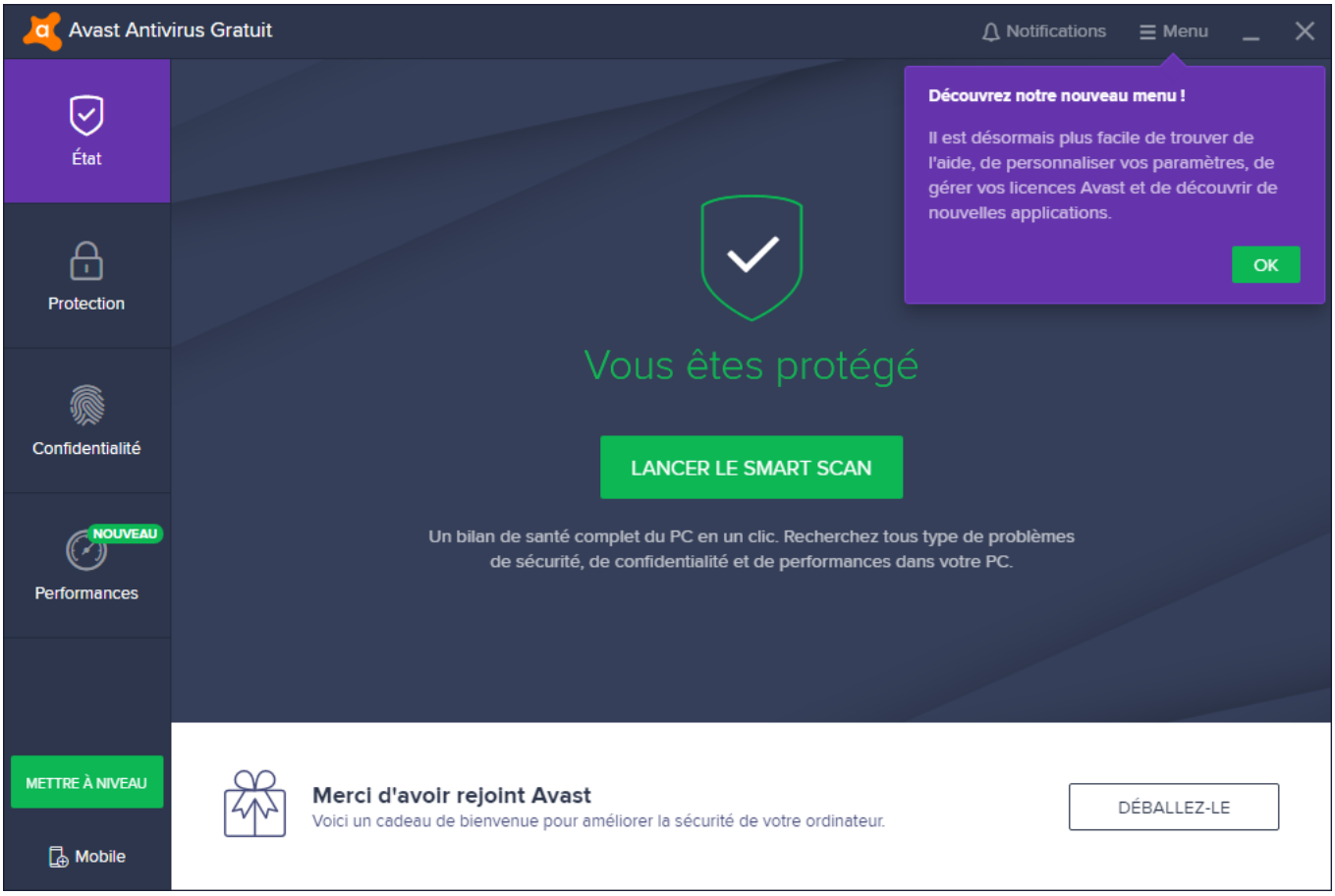
Appuyez sur **Télécharger gratuitement.** Une fenêtre de téléchargement s'affiche alors et une petite notice d'explication se charge en fond d'écran. Comme indiqué, il vous suffit de cliquer sur la fenêtre de téléchargement et appuyer sur **Enregistrer le fichier** :

Choisissez l'emplacement d'enregistrement puis cliquez sur le fichier nommé **avast_free_antivirus_setup_online.** L'installation de votre logiciel commence. Il vous suffit de suivre les indications :



Une fois l'installation lancée, une petite fenêtre en bas à droite de votre écran vous indique une jauge d'installation :

Le processus peut prendre quelques minutes. Une fois l'installation terminée, le logiciel se lance :

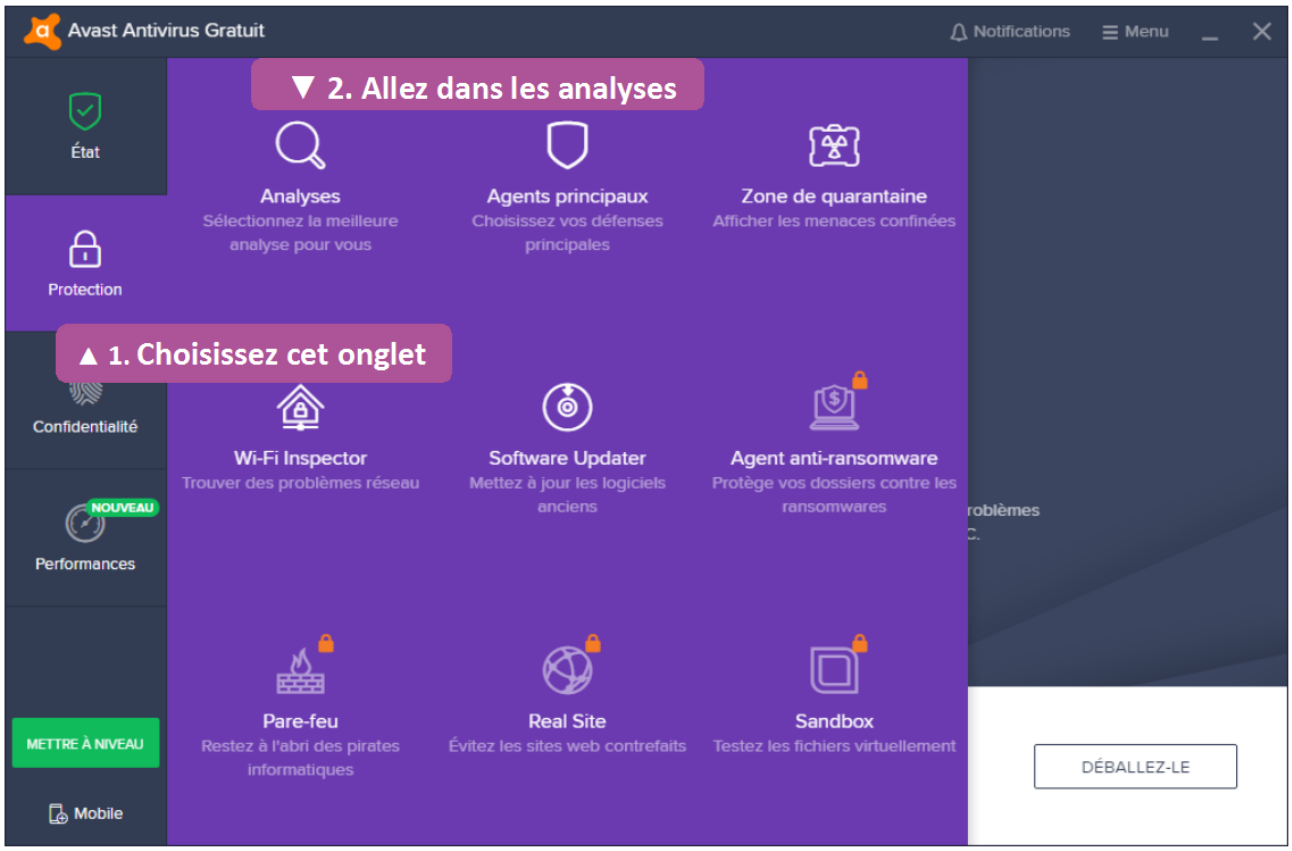


Et voila, vous avez un logiciel antivirus à jour installé sur votre ordinateur.

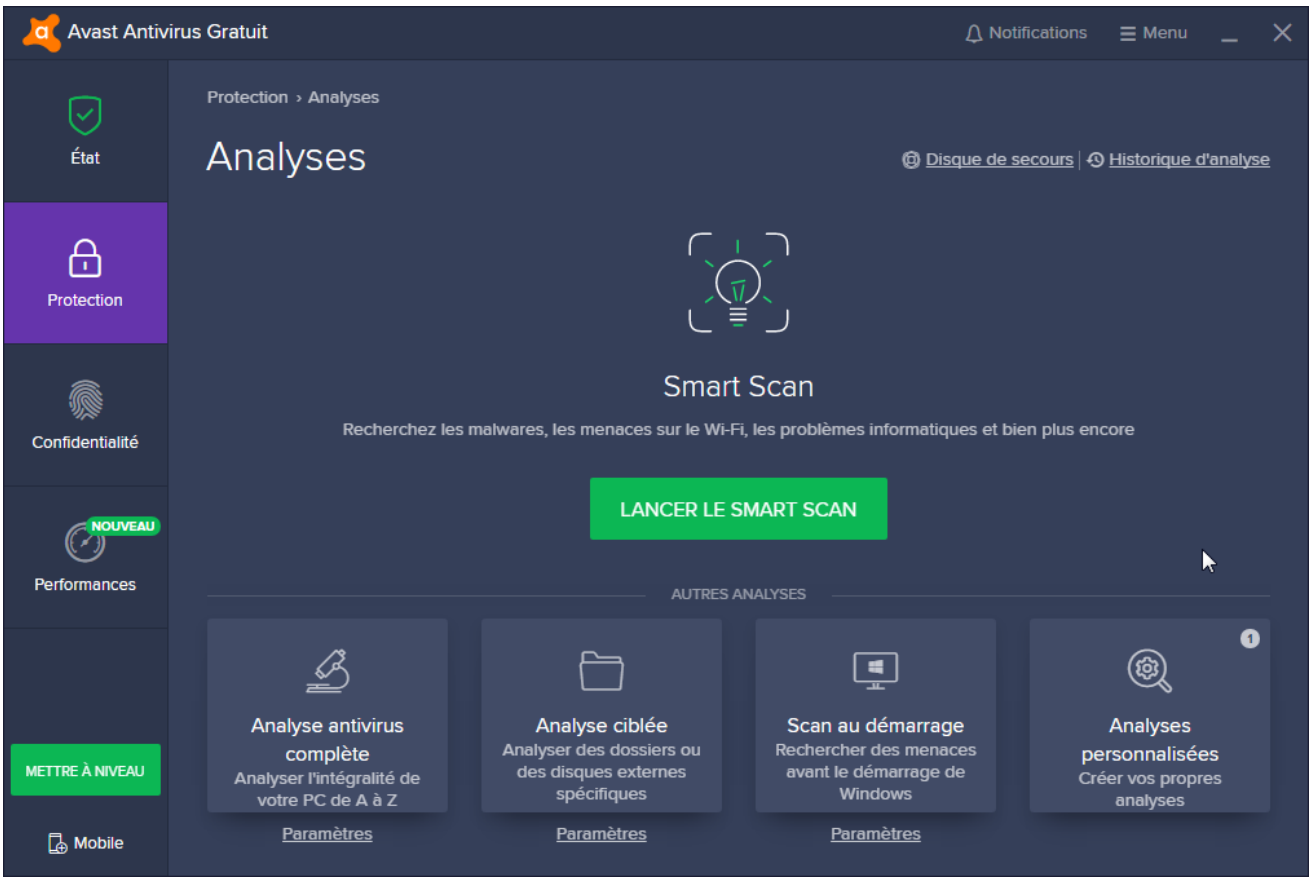
6. Scanner son ordinateur

Cependant, en version gratuite, peu d'antivirus se lancent automatiquement à la recherche des virus. Lorsqu'un logiciel se met à chercher à l'intérieur de votre ordinateur pour y trouver quelque chose, on appelle ça un **scan**.

Afin que votre machine fonctionne bien, vous devez lancer des scans Avast :

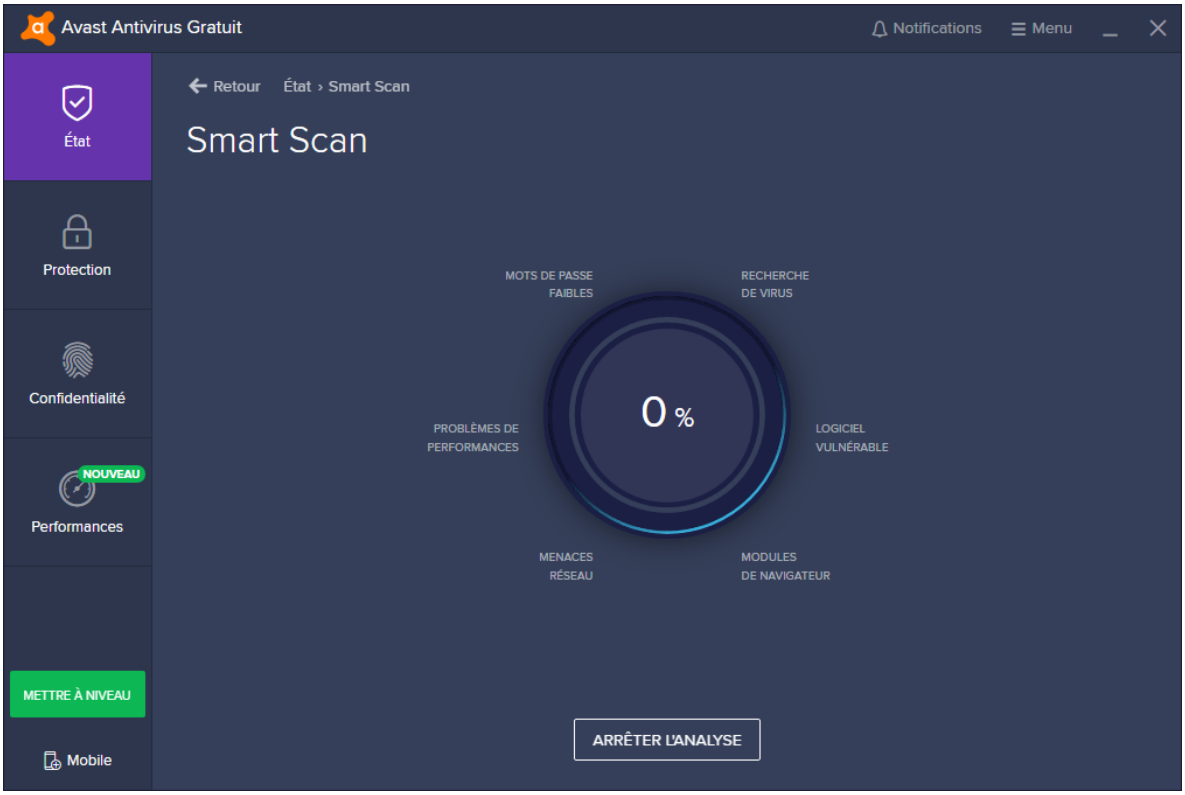


Vous avez le choix entre plusieurs types d'analyses :



- **Le smart-scan** permet de cibler les programmes et logiciels les plus vulnérables de votre ordinateur. C'est un scan rapide que vous pouvez utiliser quotidiennement (ou de façon hebdomadaire, tout dépend de votre utilisation de l'ordinateur).
- **L'analyse antivirus complète** est, comme son nom l'indique, un processus de recherche en détail afin de scanner tous les éléments de votre ordinateur. Plus longue que le smart-scan, c'est une analyse que nous vous suggérons de faire au minimum une fois par mois.
- **L'analyse ciblée** est une analyse complète mais qui ne cherche qu'à l'endroit que vous lui indiquez.
- **Le scan au démarrage** a pour but de vérifier, dès son allumage, que votre ordinateur n'est pas infecté. Cela vous évite d'avoir à le faire vous-même mais peut ralentir le démarrage de votre PC.
- **Les analyses personnalisées** vous permettent de cibler l'endroit et la nature de scan que vous souhaitez effectuer.

Une fois votre scan choisi, il vous suffit d'appuyer sur le bouton vert qui s'affiche pour le lancer :



Vous n'aurez plus qu'à suivre les instructions du logiciel selon les problèmes rencontrés.

7. Mettre son antivirus à jour

Dans les versions gratuites des logiciels, il y a rarement l'option **Mise à jour automatique** qui consiste en une recherche automatique par le logiciel des dernières versions du logiciel sur Internet. Si votre logiciel ne le fait pas, il est important que vous le fassiez vous-même manuellement.

7.1 Pourquoi ?

Les virus sont en rapide et constante évolution. Le **web** étant un réseau connecté en temps réel, la propagation de contenu y est quasiment instantanée. Les développeurs d'antivirus sont donc constamment sur le qui-vive et corrigent les failles de leurs logiciels au fur et à mesure que les virus apparaissent. Ainsi, lorsqu'une **mise à jour** est disponible, cela sous-entend qu'un correctif a été apporté au logiciel et donc, une protection supplémentaire.

7.2 Comment ?

Tout dépend de votre logiciel. Pour **Avast**, vous recevez une petite notification vous informant d'une nouvelle version du logiciel. Vous pouvez alors suivre les indications de téléchargement qui vous sont proposées.

Pour d'autres logiciels, vous devrez réinstaller le programme comme vous l'aviez fait à la première installation. La nouvelle version se calquera simplement sur la version déjà existante.

Avast vous informe lors des smart-scans, des logiciels qui ne sont plus à jour sur votre PC et vous propose de les mettre à jour à la suite du scan. Très pratique !