PÔLE D'EXCELLENCE CYBER

GUIDE PRATIQUE DE SÉCURITÉ NUMÉRIQUE

POUR LES PME/PMI, COLLECTIVITÉS ET PETITES ORGANISATIONS

V1.1

JUIN 2021

Région BRETAGNE

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

Le **Guide pratique de sécurité numérique pour les PME/PMI, collectivités et petites organisations** est constitué de 12 fiches pratiques, d'un dernier chapitre consacré à l'analyse de risque, qui est l'étape d'après, de 23 tutoriels et de 15 vidéos didactiques.

Tutoriels
Les vidéos sont sur la chaine YouTube du Pôle d'excellence cyber

Pôle d'excellence cyber

Sommaire

Avertissements : les tutoriels de ce Guide ont été réalisés sur Windows 10 Professionnel version 2004 (année=20, mois=04), version du système d'exploitation 19041.508.

Avant-propos

© Thomas Crabot

Ce guide pratique de la cybersécurité s'adresse tout autant aux responsables de collectivités locales qu'aux entrepreneurs ou collaborateurs des petites et moyennes entreprises. Il répond aux préoccupations de celles et ceux qui doivent veiller à l'intégrité de leurs équipements et installations et permet de disposer d'une boîte à outil permettant aux usagers du service public comme aux clients des petites entreprises de disposer de services sûrs et fiables et de proposer des règles simples pour réduire l'exposition aux risques cyber.

Réalisé par le Pôle d'excellence cyber avec le concours de la région Bretagne, il complète utilement le guide général réalisé par l'ANSSI et l'AMF destiné aux maires de France et responsables d'intercommunalité. Il s'adresse aux utilisateurs de base qui souhaitent sécuriser leur poste et leur environnement de travail. L'ambition est de faire de tout un chacun un citoyen français numériquement responsable.

Pour ce faire, le guide recense en 12 fiches pratiques, les réflexes et actions utiles, propose des tutoriaux et décline sur des supports vidéo à caractère pédagogique les principales opérations à mener pour renforcer son système d'information. La région Bretagne est fière du travail mené avec des utilisateurs du territoire et les experts du Pôle d'excellence cyber pour proposer ce code de la route numérique au bénéfice de tous.

Bonne lecture !

Loïg Chesnais-Girard

Président de la région Bretagne

Le présent guide est une démonstration très pratique qu'il est toujours possible de conserver le contrôle de son outil numérique, de son système d'exploitation… En tant que commandant de la cyberdéfense des armées, pour lequel la liberté d'action des forces armées dans le cyberespace est un enjeu permanent, j'apprécie tout particulièrement cette initiative.

Je note l'effort de pédagogie de ce guide au travers de ses thématiques accompagnées de tutoriels pour le rendre plus accessible encore. Cette démarche du Pôle d'excellence cyber démontre qu'il est possible pour nos petites collectivités territoriales et pour chacun d'entre nous de ne pas subir. Complémentaire des productions de l'ANSSI, il est en somme une invitation à prendre en main notre maîtrise des systèmes d'information dont nous avons désormais un besoin inévitable au quotidien. Nous savons qu'il est difficile d'avoir un personnel averti. Dans le cadre des petites entreprises, comme des petites collectivités territoriales, il relève bien de la sensibilisation et de la formation de l'ensemble des acteurs, de la conservation et l'intégrité de l'identité numérique de nos concitoyens. Sans aller plus loin dans l'analyse, je souhaite un plein succès à ce guide qui permet à chacun d'aller de l'avant dans la sécurisation de ses données. Je sais pouvoir compter sur le Pôle d'excellence cyber pour se mobiliser et répondre à vos questions, vous accompagner dans l'enjeu crucial de la sécurisation de nos données, de leur maîtrise souveraine.

Général de division aérienne Didier Tisseyre

Officier général commandant la cyberdéfense (COMCYBER)

Édito

À l'image de l'ensemble des acteurs de la vie économique, politique et sociale de la Nation, les collectivités locales s'inscrivent dans le courant de numérisation de leurs processus et services.

Elles sont soumises aux mêmes obligations de sécurisations et aux mêmes menaces cyber que tous ces acteurs et doivent cependant y apporter une plus grande attention au regard de la protection des citoyens qui leur incombe.

Cet impératif pèse sur les collectivités locales quelle que soit leur taille, qu'elles disposent ou non de ressources dédiées pour y répondre.

Le présent guide a été conçu comme un outil opérationnel à destination des élus et des personnels des collectivités locales qu'ils aient ou non des compétences informatiques et/ou de cybersécurité. Il a vocation à améliorer la sécurité numérique des collectivités locales et par la même à renforcer la ligne de participe à la défense de la Nation face à la cybercriminalité.

Il se compose du présent avant-propos destiné à éclairer la problématique générale de la sécurité numérique de 12 fiches pratiques, d'un chapitre consacré à l'analyse de risque, de 23 tutoriels et de 15 vidéos didactiques.

La sécurité numérique ne constitue pas une problématique entièrement nouvelle en matière de sécurité, seul le support numérique est nouveau et apporte les spécificités propres débouchant en particulier sur la cyber-criminalité puisqu'il s'agit de celui des systèmes d'informations (équipements, réseaux,...).

Les questions posées par la sécurité numérique sont identiques à celles prises en charge par les collectivités locales dans la cadre de la sécurité globale de leur entité. L'objectif de la sécurité numérique est de protéger des actifs immatériels (données et traitements) créés, exploités, valorisés et archivés sur des supports informatiques.

Les buts visés par les acteurs malfaisants sont le vol (vol de données, vol financier, escroquerie,...) et le sabotage (interruption du service, destruction de données, destruction d'applications,...).

De façon synthétique, un système d'information est constitué :

- d'équipements physiques (serveurs informatiques, poste de travail, tablettes, portables de tous types, équipements de stockage externes - disque dur, clé USB,...-) et d'équipements de réseau (réseau local, réseau distant),
- de traitements informatiques (système d'exploitation destinés au fonctionnement des équipements, applications générique du type bureautique, applications métiers - paie, comptabilité, gestion d'un service,...-),
- de données qui constituent le capital immatériel de l'entité propriétaire.

Pour la collectivité locale, la mise en œuvre de la sécurité numérique doit débuter par une analyse préalable qui intègre la gestion des risques. Il n'existe pas de risque zéro, c'est pourquoi, le guide porte une attention particulière à l'analyse des risques dont l'objet majeur est de définir le risque résiduel accepté par la collectivité en fonction des ressources affectées à la sécurisation.

L'analyse des risques permet ainsi de définir les éléments du système d'information dont la collectivité locale doit assurer la sécurisation parce qu'elle en est propriétaire.

En effet, la collectivité locale peut utiliser des systèmes d'information en tant qu'usagère dont elle n'est pas propriétaire, qui sont implantés à distance et dont elle ne peut assurer la sécurisation exhaustive (gestion des transports scolaires par exemple).

Les éléments qui relèvent en tout état de cause de la collectivité locale sont :

- La sécurisation des locaux dans lesquels sont implantés des équipements de système d'information : serveur et réseau local associé (s'ils existent), postes de travail, équipements de stockage… Ce point traite notamment de la sécurisation des accès, de la sécurité incendie, de la prévention des risques naturels (inondations,…).
- La sécurisation des équipements : fixation des postes de travail, stockage des équipements non utilisés.
- La sécurisation des accès aux équipements. Ce point est central pour la sécurité numérique, il traite de la gestion des mots de passe qui sont les clés d'accès aux données (si la porte est ouverte !). Une gestion rigoureuse des mots de passe sur les postes de travail et les périphériques de type tablette est la première obligation : sans elle pas de sécurité numérique. Un point d'attention, le responsable de la collectivité locale doit informer chaque agent à qui il confie un moyen d'accès au système d'information que le mot de passe qu'il définit n'est pas sa propriété et qu'il doit le communiquer en cas d'absence ou de départ. La gestion des cessions est impérative.
- La sécurisation des accès aux applications dont la collectivité est propriétaire. Cette sécurisation est assurée par la gestion des habilitations (saisie et modification ou lecture seule).
- La conservation des données dont la collectivité est propriétaire. Les données sont conservées dans le strict respect des dispositions du RGPD (Règlement Général de Protection des Données), des règles légales de durée de conservation et d'archivage.
- La sauvegarde des données dont la collectivité est propriétaire. Cette opération vise à assurer la continuité de l'action de la collectivité locale en cas de vol ou de destruction des données. La périodicité des sauvegardes et la sécurisation des lieux de stockage (jamais dans le même local que les données actives du système d'information) sont à définir de façon impérative.
- La sauvegarde des applications métiers, cette sauvegarde concerne les applications développées par la collectivité locale pour un usage propre, elle s'applique aux programmes. Chaque version doit être sauvegardée, la sécurisation des lieux de stockage est identique au point précédent.

La lecture et la mise en œuvre des dispositions du présent guide permettent de formaliser un dossier de sécurité numérique de la collectivité locale* qui apporte une garantie aux élus, aux personnels et aux citoyens sur la prise en charge de la cybersécurité et de la lutte contre la cybercriminalité, ce qui est essentiel pour la confiance accordée à la numérisation.

Le Pôle d'excellence cyber espère que ce guide facilitera la réalisation de cet objectif fondamental pour la sécurisation numérique des collectivités locales, bonne lecture !

Philippe Verdier

Président du Pôle d'excellence cyber

* À titre d'exemple, ce dossier doit comprendre les éléments suivants qui le rendent éligibles aux contrôles prévus par les dispositifs légaux et règlementaires.
- L'intitulé de la collectivité locale, le nom de son responsable légal, les noms des personnes ayant éventuellement reçu délégation pour la gestion de la sécurité numérique.
- La liste des équipements (serveurs, poste de travail, tablette, portables,…) avec leur caractéristiques (modèle, date d'acquisition, nom des personnes les ayant installés) et les personnes habilitées à les utiliser (attention au risque lorsqu'un même équipement est accessible par plusieurs utilisateurs, instituer un fichier d'utilisation : qui ? à quel moment ? Et rendre la fermeture de cession impérative entre deux utilisateurs).
- La description des locaux où sont installés ou stockés les équipements avec la description des moyens de sécurisation mis en œuvre (portes, armoires sécurisés,…).
- Un fichier des changements de mot de passe d'accès aux équipements (permet de faire respecter la périodicité, le fichier est signé par l'utilisateur à chaque changement de passe, il ne comporte évidemment pas les mots de passe.
- Un fichier des droits d'accès aux applications dont la collectivité est propriétaire, ce fichier établit par application donne le nom des personnes habilitées à l'accès (préciser si nécessaires les types d'habilitation : saisie modification des données, simple consultation) et la durée d'habilitation. Il permet notamment de gérer les départs et les arrivées de personnes.
- Un fichier par application décrivant les règles de conservation et d'archivage des données. Ce fichier décrit les modalités de destruction des données.
- Un document d'organisation des sauvegardes des données et des applications : description de la périodicité des sauvegardes, définition des supports de stockage et de leur lieu conservation.
- Un fichier de gestion des droits d'accès à la messagerie de la collectivité territoriale.
- Un fichier des droits d'accès à internet.

12

FICHES PRATIQUES _

N°1

Fiche n°1

Données personnelles et RGPD

Les collectivités territoriales ont une longue expérience de la gestion des données publiques, elles sont de véritables sanctuaires de données, qu'elles conservent parfois pendant une durée illimitée (cas de l'archivage définitif). Il en va de même pour les autres organisations. Entré en vigueur le 25 mai 2018, le Règlement Général sur la Protection des Données (RGPD) impose à tous les organismes de respecter certaines règles qui visent à protéger les données à caractère personnel confiées par les administrés aux gestionnaires des applications dont ils sont les utilisateurs et/ou les usagers. Le respect de ce règlement est une condition essentielle pour mieux protéger les citoyens, un facteur de transparence et de confiance à leur égard. Ce règlement est aussi une garantie de sécurité juridique pour les élus et les dirigeants d'entreprises, qui sont responsables des données utilisées et stockées au sein de leur organisation.

Certains éléments de cette fiche sont issus du site Internet de la Commission nationale de l'informatique et des libertés (CNIL)[1], l'autorité référente et de contrôle en France en charge des questions de protection des données.

Les données à caractère personnel

L'Article 4 du RGPD indique que les **données à caractère personnel** sont toutes les informations se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement. Par exemple, un nom, une photo, une empreinte, une adresse postale, une adresse électronique, un numéro de téléphone ou de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, etc. Ces éléments sont régulièrement utilisés par les applications des systèmes d'information des organisations en contact avec le public, pour toute opération qui concerne une personne physique, et font l'objet d'un traitement quotidien (collecte, conservation, modification, consultation, diffusion, effacement, etc.) au sein de celles-ci. Ces données peuvent être recueillies à l'oral ou via un formulaire et figurer dans divers documents numériques gérés par les agents, par exemple les fichiers qui sont issus de ressources humaines, d'un téléservice, de la vidéosurveillance.

Les données sensibles : un cas particulier des données à caractère personnel

L'Article 9 du RGPD fait le point sur une catégorie particulière de données à caractère personnel, appelée **données sensibles**. Il s'agit de données qui révèlent, directement ou indirectement, l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales des personnes, les données génétiques et biométriques ou encore celles qui sont relatives à la santé ou l'orientation sexuelle. Par exemple, les dossiers contenant des données de santé, y compris les dossiers enfants avec une partie médicale ou les données utiles pour les demandes d'aide au logement en lien avec le handicap.

1 https://www.cnil.fr/professionnel

Attention à bien distinguer « données sensibles » et « données sensibles au sens de la Loi ». En effet, une confusion apparaît souvent entre les données qui sont sensibles pour une organisation (celles qui ont trait à l'organisation interne, les données financières, des dossiers politiquement et médiatiquement sensibles, etc.) ou qui sont considérées sensibles par les agents (certaines données sociales, les mariages entre personnes d'un même sexe[2], etc.), mais qui ne sont pas nécessairement des données sensibles au sens du Règlement et de la Loi Informatique et Liberté et ne sont pas soumis au même régime juridique.

Avant de recueillir des données sensibles, l'organisation doit s'assurer qu'elle rentre bien dans l'un des cas légitimes suivants R1 :

- La personne concernée a donné par écrit son consentement explicite ;
- Les données sont rendues publiques par la personne concernée ;
- Les données doivent servir pour des recherches médicales ou à la sauvegarde de la vie humaine ;
- L'utilisation des données est justifiée par l'intérêt publique et autorisée par la CNIL ;
- Les données appartiennent à des membres d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

Les étapes à suivre pour se mettre en conformité au RGPD

Chaque organisation doit apporter la preuve[3] de sa conformité au règlement auprès de l'autorité de contrôle (CNIL). Les étapes suivantes permettront aux organisations de se mettre en conformité au RGPD :

- **Désignez une personne déléguée à la protection des données (DPO) et notifiez-le à la CNIL** R2 **:** il peut s'agir d'une personne physique ou morale, interne à l'organisation ou externe. Il est également possible de mutualiser cette fonction de délégué entre plusieurs institutions. Dans ce cas, les organisations ont l'obligation de conclure une convention de mutualisation. Enfin, le délégué doit être en mesure d'exercer ses fonctions et missions en toute indépendance (ne pas être juge et partie). Par exemple, les conseillers municipaux (dont le maire) ne peuvent pas être désignés délégués, car ils prennent directement part au processus de décision concernant les fichiers mis en œuvre dans leur organisation.

Vous devez obligatoirement notifier à la CNIL la désignation de votre délégué en utilisant le téléservice https://www.cnil.fr/designation-dpo.

2 Bien que l'orientation sexuelle entre dans la catégorie des données sensibles, la publication d'un mariage homosexuel, qui donne clairement une telle indication, doit être légalement rendue public. Une telle indication n'est pas une donnée sensible au regard de la Loi (« Étude pour le CREOGN : Données personnelles et collectivités territoriales : usages actuels et recommandations »).

3 https://www.cnil.fr/fr/documenter-la-conformite

- **Constituez et maintenez à jour les registres exigés par le RGPD R3 :**
  - **a. Le registre listant les traitements de données :** ce registre permet d'avoir une vision claire et globale des activités de l'organisation qui nécessitent la collecte et le traitement de données personnelles. Appuyez-vous sur le modèle de registre proposée par la CNIL[4] ;
  - **b. Le registre des violations de données à caractère personnel :** l'organisation doit recenser l'ensemble des éléments relatifs aux violations[5], par exemple la perte d'une clé USB non chiffrée contenant des données personnelles, l'envoi accidentel d'un courriel contenant des informations qui concernent une autre personne, l'accès malveillant à une base de données. Notez que **l'historique des violations de données peut être consigné dans** le registre listant les traitements de données.

L'organisation est dans l'obligation d'informer la CNIL dans les 72 heures après un incident de violation des données personnelles, voire la personne concernée si cette violation entraîne un risque élevé. Cette notification s'effectue en ligne sur le site de la CNIL[6].

- **Faites le tri dans vos données R4.** Pour chaque fiche du registre listant les traitements de données, vérifiez :
  - **a. La pertinence et la nécessité des données traitées : par exemple, si vous n'offrez aucun service ou aucune rémunération attachés au fait que vos salariés aient des enfants, cette donnée ne vous est pas utile ;**
  - **b. La nature des données traitées :** le RGPD interdit le recueil et l'exploitation des données sensibles. **Si l'organisation recueille de telles données, elle doit s'assurer d'en avoir le droit (voire la recommandation R1)** ;
  - **c. Les accès aux données :** seuls les agents habilités peuvent avoir accès aux données. Ces accès doivent correspondre à un besoin réel et être en lien avec l'exercice de leurs missions ;
  - **d. La durée de conservation et d'archivage des données : la CNIL et le Service Interministériel des Archives de France (SIAF) ont élaboré des outils d'aide à l'identification des durées applicables à la conservation des données, ainsi qu'un guide pour faciliter la mise en œuvre de ce principe[7].**

- **Respectez le principe de transparence et les droits des administrés R5 :**
  - **a.** Chaque fois que des données personnelles sont recueillies, l'organisation doit informer en toute transparence les personnes concernées des conditions d'utilisation de leurs données et de leurs droits. Pour cela, les supports utilisés (formulaire, questionnaire, site Internet, etc.) doivent comporter des mentions d'information. Appuyez-vous sur les exemples de mentions[8] qui sont proposés par la CNIL ;

4 https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement
5 https://www.cnil.fr/fr/les-violations-de-donnees-personnelles
6 https://notifications.cnil.fr/notifications/index
7 https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees
8 https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation

b. Donnez les moyens effectifs d'exercer effectivement leurs droits aux administrés, par exemple, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée sur votre site Internet. l'organisation doit répondre dans les meilleurs délais (1 mois au maximum) aux demandes de consultation, de rectification ou de suppression des données[9].

- **Sécurisez les données** R6 **:** contre les accès non autorisés, contre les modifications non désirées, contre le vol ou la destruction. L'organisation est tenue à une obligation légale d'assurer la sécurité des données personnelles qu'elle détient. Toutes les mesures pouvant permettre de mener à bien cette mission doivent être prises :

a. La sécurité physique : sécurisation du site, des locaux, des armoires, etc. ;

b. La sécurité informatique : poste du travail, applications, supports amovibles, droits d'accès informatiques (les agents doivent disposer d'un identifiant individuel et d'un mot de passe personnel, complexe, et régulièrement mis à jour), etc.

Appuyez-vous sur l'ensemble des mesures et recommandations listées dans les différentes fiches de ce Guide, en vous aidant aussi des tutoriels et des vidéos qui sont à votre disposition.

- **Encadrez la sous-traitance** R7 **:** l'organisation peut confier le traitement des données à caractère personnel qu'elle détient à des prestataires. Dans ce cas, elle doit s'assurer du bon traitement de ses données par ses sous-traitants, dans le strict cadre du règlement RGPD. Le contrat avec la société sous-traitante doit inclure plusieurs mentions particulières obligatoires[10]. Vous trouverez aussi des clauses supplémentaires à inclure dans le contrat de sous-traitance dans la fiche 12 «Externalisation».

Le RGPD consacre une logique de responsabilisation de tous les acteurs impliqués dans un traitement de données personnelles en y incluant les sous-traitants. Ils doivent donc aussi participer à la mise en conformité des organisations territoriales, en les aidant, sous peine de sanctions s'ils le refusent, à satisfaire aux exigences du RGPD.

- **Réalisez une analyse d'impact relative à la protection des données (AIPD)** R8 **:** mener une AIPD est obligatoire pour tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes concernées. Des critères précis existent, vous les trouverez sur le site de la CNIL[11], ils permettent de déterminer si votre traitement est susceptible d'engendrer des risques élevés. La CNIL a également élaboré une méthode, un catalogue de bonnes pratiques et un outil, PIA, qui vous aideront à mener une AIPD[12] et à déterminer les mesures proportionnelles aux risques identifiés qui doivent être prises.

9 https://www.cnil.fr/fr/respecter-les-droits-des-personnes
10 https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article28
11 https://www.cnil.fr/fr/gerer-les-risques
12 https://www.cnil.fr/fr/RGPD-analyse-impact-protection-des-donnees-aipd

N°1

- **Protégez-vous contre les pratiques abusives liées à la mise en conformité au RGPD** R9 **:** certaines sociétés démarchent les professionnels, parfois de manière agressive, afin de vendre un service d'assistance à la mise en conformité au RGPD. Dans certains cas, il peut même s'agir de manœuvres pour collecter des informations sur l'organisation en vue d'une escroquerie ou d'une attaque informatique. Au regard de pratiques commerciales trompeuses constatées, la DGCCRF et la CNIL ont formulé plusieurs recommandations que vous pouvez consulter en ligne[13]. La DGSI, le CISSE ou la Gendarmerie peuvent aussi vous éclairer sur la réputation de ces acteurs.

Afin d'accompagner les collectivités territoriales dans leur mise en conformité au RGPD, la CNIL a élaboré un guide de sensibilisation disponible sur son site Internet[14].

Dans la même optique, le syndicat mixte de coopération territoriale, Mégalis Bretagne, ainsi que la Ville de Saint-Avé ont mis en place le site www.openrgpd.fr. Vous y trouverez divers outils et tutoriels, notamment l'outil OpenRGPD qui vous permettra de réaliser un recensement des traitements de votre collectivité et d'en extraire un **registre** ; le Kit Méthodologique Mégalis Bretagne est une véritable boite à outils pour aider les collectivités à mener à bien leur mise en conformité ; enfin le jeu RGPD GAME permettra de sensibiliser les agents des collectivités.

La plateforme Mairie 2000[15] offre aux élus la possibilité du suivre le cours en ligne « La mise en œuvre du RGPD par les collectivités ».

Vous trouverez aussi sur le site de l'ANSSI un « kit de la sécurité des données »[16], mis à disposition de toutes les organisations, qui rassemble de nombreux documents qui pourraient compléter les dispositifs cités plus haut.

Cette fiche contient 9 recommandations.

13 https://www.economie.gouv.fr/files/files/directions_services/dgccrf/presse/communique/2018/CP_CNIL_DGCCRF_RGPD20180612.pdf
14 https://www.cnil.fr/sites/default/files/atoms/files/cnil-guide-collectivite-territoriale.pdf
15 https://moocmairie2000.fr/moodle/
16 https://www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel/

Fiche n°2

Poste de travail

Le poste de travail constitue le vecteur d'accès aux traitements et par la même aux données utilisées par les traitements qui constituent le capital immatériel des systèmes d'information. Sa protection est un élément majeur de la cybersécurité. Un poste de travail non sécurisé est une porte ouverte qui rend illusoire la sécurisation de tout autre élément des architectures des SI.

Lorsque vous démarrez votre ordinateur pour la première fois, ou que vous réinstallez votre système, un compte avec des droits « administrateur » se crée. Quelle que soit votre système d'exploitation, la première chose à faire pour sécuriser votre ordinateur est de créer un **compte avec des droits limités** R1. Dans Microsoft Windows cette session s'appelle « utilisateur standard » (voir le tutoriel « Créer un compte utilisateur standard »). Les comptes standards peuvent utiliser la plupart des logiciels et modifier les paramètres du système sans toutefois affecter la sécurité de votre ordinateur, ni les sessions des autres utilisateurs.

Nous recommandons de **ne pas vous connecter à votre système à l'aide d'un compte Microsoft** R2 (voir le tutoriel « Se connecter à Windows 10 avec un compte local »). En utilisant ce service, certains paramètres de votre ordinateur (y compris les mots de passe) seront stockés sur les serveurs appartenant à Microsoft. En outre, ce type de compte est connecté aux nombreux services Microsoft qui collectent et envoient vos données personnelles à Microsoft, ses filiales et ses partenaires.

Pour les organisations qui ont un administrateur pour leur SI et leur infrastructures, qui gère les comptes des utilisateurs à l'aide d'un annuaire, tel Active Directory, **la sécurisation des annuaires, ainsi que la vérification régulière du niveau de leur sécurité est primordiale** R3. En effet, les annuaires contiennent les informations d'identification des utilisateurs, ils constituent donc des cibles privilégiées pour des personnes malveillantes. L'administrateur système et réseaux et/ou les personnes en charge de la sécurité des systèmes d'information peuvent se référer à la note technique proposée par l'ANSSI, « Recommandations de sécurité relatives à Active Directory »[17] et à la liste des points de contrôle Active Directory[18]. Notons enfin que le poste de travail de l'administrateur doit être bien protégé et doit faire l'objet d'une surveillance toute particulière.

Les recommandations élémentaires pour sécuriser son système et sa session de travail :

- **Installez un logiciel anti-virus et un pare-feu** R4 **:** téléchargez chaque programme sur le site officiel de son éditeur. Vous pouvez vous référez à la liste des logiciels libres proposée par le **Socle Interministériel de Logiciels Libres**[19] ou utiliser un éditeur propriétaire, tel Windows Defender qui est fourni avec votre PC, ou l'un des principaux antivirus du marché, sachant qu'il est aussi recommandé d'en changer régulièrement. Analysez votre ordinateur régulièrement, ou à la moindre alerte, à l'aide de votre antivirus. N'installez pas plusieurs antivirus sur votre ordinateur. Toutefois, lorsque

17 https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf
18 https://www.cert.ssi.gouv.fr/uploads/guide-ad.html
19 https://sill.etalab.gouv.fr/fr/software

vous avez un soupçon quant au bon fonctionnement de votre ordinateur, vous pouvez avoir recours à des outils complémentaires, telles les analyses antivirus en ligne ou les logiciels anti-spywares proposés par des éditeurs connus (citons Kaspersky Virus Removal Tool, Malwarebytes, Scanner anti-rootkit Sophos). Une fois l'analyse effectuée, prenez la précaution de désinstaller ces outils (voir le tutoriel « Désinstaller les applications »).

Afin d'être plus efficace dans votre défense, nous vous conseillons d'utiliser des solutions antivirus différentes pour les serveurs d'infrastructures et pour les postes clients.

- **Déconnectez-vous de votre session dès que vous vous éloignez de votre ordinateur, même si ce n'est que quelques minutes** R5 **:** c'est un moyen facile d'empêcher une personne curieuse ou malveillante d'accéder à votre système et vos données (voir le tutoriel « Fermer la session »).

- **Activez le verrouillage automatique de votre session** R6 : ainsi, si vous oubliez de vous déconnecter, le système le fera à votre place au bout d'un temps déterminé, idéalement le plus court possible, quelques minutes en général. Une fois déconnecté vous devrez remettre votre mot de passe pour accéder à nouveau à votre session (voir le tutoriel « Verrouiller automatiquement la session »).

- **Installez les mises à jour du système d'exploitation et activez la vérification automatique des mises à jour** R7 **:** les mises à jour critiques ou de sécurité doivent être installées sans délai, elles sont signalées par des messages de votre système d'exploitation. Il faut donc penser à redémarrer son poste de travail **au moins une fois par semaine**, et de préférence le mercredi matin (car c'est tous les deuxièmes mardis de chaque mois que Microsoft propose ses mises à jour, le *Patch Tuesday* ou *Update Tuesday*).

- **Mettez à jour tous les programmes et applications installés sur votre ordinateur** R8 **:** avant même d'utiliser un logiciel, vous devez vérifier que celui-ci est bien à jour. En effet, un logiciel non mis à jour constitue une porte d'entrée pour les attaquants. Si le logiciel que vous utilisez ne propose pas cette option dans ses paramètres par défaut, vous devez l'activer.

- **Faites des sauvegardes régulières de vos données et sauvegardez votre système d'exploitation** R9 **:** avoir à disposition des sauvegardes à jour est un moyen efficace de réduire la menace des rançongiciels (voir la fiche 9 « Plan et stratégie de sauvegarde »).

- **Désactiver vos périphériques lorsque vous ne les utilisez pas** R10 **:** par exemple, les outils tels le microphone et la camera. Vous pouvez aussi utiliser des caches camera frontale sur vos téléphones et tablettes car il est généralement compliqué de les contrôler ou de les désactiver.

- **Désactivez les services de connexion non nécessaires à votre métier** R11 **:** tels que le Bluetooth, le Wi-Fi, la 4G, etc. Si vous les utilisez de temps à autre,

ne les activez alors que lorsque vous en avez besoin, car laisser toutes ces possibilités de connexion ouvertes en permanence rend vos appareils plus vulnérables aux cyber-attaques.

Quelques recommandations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10 :

- **Désactivez la géolocalisation de votre ordinateur, téléphone, tablette, montre connectée** R12**.** Cet outil de sécurité et de surveillance inclus dans de nombreuses applications (mise en relation de personnes, assistance à la navigation, montres ou cameras connectées, gestion en temps réel des déplacements, etc.) est très intrusif[20]. La législation française interdit de collecter des informations privées par le biais de la surveillance sans le consentement explicite de la personne. De plus, avec la pratique d'Apportez Votre Équipement personnel de Communication (AVEC, BYOD en anglais), il est difficile de déterminer la frontière entre ce qui relève de la sphère privée ou de la sphère professionnelle. L'article L. 1121-1 du Code du travail, dit que «nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché». L'employeur qui souhaite mettre en place un dispositif de géolocalisation dans l'organisation doit informer et consulter les représentants du personnel et informer ses collaborateurs.

- **Désactivez les services d'informatique en nuage (*Cloud*) intégrés au système d'exploitation** R13, par exemple OneDrive de Microsoft, DropBox de Mac OS. Dès que vous stockez des données sur un service *Cloud*, qui synchronise vos données avec des serveurs distants, il faut bien vous assurer des mesures contractuelles. En effet, les serveurs *Cloud* peuvent faire l'objet d'un piratage, ils ont généralement une capacité limitée lorsqu'ils sont gratuits, et le risque d'exploitation commerciale de vos données, ou à des fins d'espionnage, est important. Attention aussi à bien avoir tout le temps accès à vos données, et assurez-vous de bien les récupérer en fin de contrat.

- **Durcissez les paramètres de personnalisation de l'expérience utilisateur** R14 **:**
  - Désactivez l'identifiant unique de publicité : cet identifiant permet de détecter votre appareil de manière unique, ce qui permet à Microsoft et aux annonceurs d'afficher de la publicité ciblée ;
  - Désactivez l'assistant personnel virtuel intégré au système d'exploitation : par exemple Cortana dans Microsoft, ou Siri dans Mac OS et iOS. Ces logiciels récoltent des informations sensibles qui vous concernent et peuvent les divulguer : votre localisation géographique et vos emplacements habituels, votre historique de recherche, vos centres d'intérêt, vos contacts, vos rendez-vous, les informations de certaines applications (Santé), etc.

Pour appliquer certains de ces conseils relatifs au respect de la vie privée et à la confidentialité des données sous Windows 10, vous pouvez vous appuyer sur des tutoriels suivants : «Désactiver la localisation», «Désactiver l'identifiant unique de publicité», «Désactiver Cortana», «Désactiver OneDrive et supprimer les documents stockés en ligne».

20 https://www.frandroid.com/culture-tech/securite-applications/515849_dgse-mi6-nsa-une-application-fitness-trahit-lidentite-de-militaires-et-despions

N°2

Les organisations qui souhaitent déployer ces mesures de sécurité dans un environnement Active Directory, peuvent se référer au guide « Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10 »[21] proposé par l'ANSSI.

Cette fiche contient 14 recommandations.

Références :
https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
https://www.ssi.gouv.fr/uploads/2017/01/np_securisation_windows10_collecte_de_donnees_v1.2.pdf
https://www.cnil.fr/fr/securite-securiser-les-postes-de-travail
https://www.cnil.fr/fr/reglez-les-parametres-vie-privee-de-windows-10

21 https://www.ssi.gouv.fr/uploads/2017/01/np_securisation_windows10_collecte_de_donnees_v1.2.pdf

Fiche n°3

Mots de passe

Ordinateur personnel, messageries électroniques, sites en ligne, logiciels métiers, etc., les mots de passe constituent la première ligne de protection des comptes utilisateurs. Un mot de passe mal choisi ou mal protégé peut compromettre la sécurité de vos accès, et donc de l'ensemble de votre système d'information. Il incombe donc à tous les agents, aux prestataires et fournisseurs ayant accès au système d'information de l'organisation, de prendre les mesures appropriées pour bien choisir et sécuriser leurs mots de passe.

Voici les bonnes pratiques à adopter pour gérer efficacement vos mots de passe :

- **Bien choisir son mot de passe** R1 **:** un mélange aléatoire de lettres majuscules et minuscules, de chiffres et des caractères spéciaux, suffisamment long, d'au moins 15 caractères. Le choix d'un mot de passe doit aussi se faire au regard de la criticité du service, le mot de passe administrateur d'une application ou d'un équipement sera considéré comme étant très critique, il sera donc plus long et plus complexe encore. Votre messagerie électronique doit également être considérée comme un service critique, car votre adresse électronique est généralement associée à de nombreux comptes en ligne.

Les mots de passe à bannir :

- Un mot ou une combinaison des mots d'un dictionnaire, une phrase prise dans un livre (même longue) ;
- Une chaîne de caractères basée sur les lettres adjacentes de votre clavier : azerty, qwerty, 123456, etc.
- Un mot de passe qui contient des informations personnelles ou qui peuvent être facilement devinées : date de naissance, prénom de votre enfant, etc.
- Enfin, faites également attention à ne pas utiliser des variations de ces mauvais exemples de mots de passe, par exemple, en remplaçant la lettre « o » par « 0 » (zéro) ou en ajoutant un caractère spécial à la fin d'un mot du dictionnaire, car toutes ces variantes usuelles sont répertoriées dans des « dictionnaires de mots de passe », facilement téléchargeables sur Internet et utilisés par les pirates.

Un outil en ligne qui vous aide à construire un mot de passe fort et simple à retenir est disponible sur le site de la CNIL[22]. Vous pouvez également tester à la suite la robustesse de celui-ci sur le site de l'ANSSI[23].

22 https://www.cnil.fr/fr/generer-un-mot-de-passe-solide
23 https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe/

- **Utilisez un mot de passe unique pour chaque service** R2 **:** en particulier, les mots de passe de votre messagerie électronique personnelle et professionnelle doivent être différents. Il peut être tentant d'utiliser le même mot de passe pour tous vos comptes, afin de ne pas avoir à mémoriser une multitude de données. Cependant, en cas de perte ou de vol de votre mot de passe, tous vos comptes peuvent être impactés.

N'utilisez jamais le mot de passe de votre messagerie électronique pour vous inscrire sur un site en ligne. Les sites Web sont sujets à de très nombreuses attaques informatiques et par conséquent à des fuites de données massives. Il existe des outils en ligne, comme haveibeenpwned.com[24] ou Firefox Monitor[25], qui recensent les comptes de messageries électroniques qui ont été compromis à l'occasion de fuites massives de données. En entrant votre adresse électronique, vous pouvez ainsi savoir si elle figure dans l'une des bases de données qui ont été piratées, quel site est à l'origine de la fuite, et si votre mot de passe ou d'autres données vous concernant sont potentiellement entre les mains de personnes malveillantes (voir le tutoriel « Vérifier si une fuite de données en ligne vous concerne »).

- **Protégez vos mots de passe** R3 **:** ne les stockez pas dans un fichier texte non chiffré, ni sur un papier que vous laisseriez trainer aux alentours de votre ordinateur (un post-it sous votre clavier, etc.). Ne partagez pas vos mots de passe dans un message électronique, ou par téléphone, même si vous échangez avec une personne de confiance. N'ouvrez pas vos sessions sur des ordinateurs partagés ou des machines qui ne vous appartiennent pas. Évitez d'utiliser l'option, qu'offrent la plupart des navigateurs, qui propose d'enregistrer vos mots de passe. Une alternative consiste à utiliser un gestionnaire de mots de passe qui vous aide à générer des mots de passe robustes et différents pour chaque compte, et qui permet de les stocker de manière chiffrée (voir le tutoriel « Gestion des mots de passe avec KeePass »).

Lorsque vous utilisez un compte local dans Windows 10, vous pouvez créer un disque de réinitialisation de mot de passe à l'aide d'une clé USB. Ainsi, si vous oubliez votre mot de passe, vous pourrez le réinitialiser (voir les tutoriels « Créer un disque de réinitialisation de mot de passe pour un compte local » et « Réinitialiser le mot de passe oublié d'un compte local »).

- **Changez régulièrement vos mots de passe** R4 **:** cela permet d'éviter un certain nombre de dangers. Parfois, il peut être difficile de savoir si quelqu'un d'autre a accès à vos comptes; par exemple, une personne qui a réussi à pirater votre messagerie peut y accéder pendant une longue période pour surveiller vos données; vous avez aussi pu enregistrer vos mots de passe sur un ordinateur qui ne vous appartient plus. Renouvelez donc vos mots de passe avec une fréquence raisonnable (tous les 2 ou 3 mois), lorsque vous changez de matériel, ou au moindre soupçon, et surtout **à partir d'un ordinateur sain** (voir la fiche 2 : « Poste de travail »). Pensez également à supprimer les accès des agents qui partent en retraite, des agents mutés, des anciens stagiaires ou des anciens sous-traitants, et modifiez les mots de passes des services auxquels ces anciens collaborateurs avaient accès[26].

24 https://haveibeenpwned.com
25 https://monitor.firefox.com/
26 https://docs.microsoft.com/fr-fr/microsoft-365/admin/add-users/remove-former-employee?view=o365-worldwide

- **Faites attention aux indices de mots de passe ainsi qu'aux réponses aux questions secrètes** R5 **:** lorsque vous créez un compte personnel en ligne ou sur votre ordinateur, il arrive que l'on vous demande de fournir un indice sur votre mot de passe pour vous aider à vous en rappeler. Ne donnez surtout pas d'indices qui permettrait de deviner facilement votre mot de passe. De la même manière, lorsque l'on vous demande de répondre aux questions secrètes afin de pourvoir réinitialiser votre mot de passe au cas où vous l'auriez oublié, évitez de faire des réponses trop évidentes aux questions. Un pirate aurait, par exemple, une forte probabilité de deviner avec succès la réponse à la question « Quelle était votre première voiture ? ». Nous vous recommandons de ne jamais faire de réponse trop courte (un seul mot), et de préférer au final utiliser là aussi un mot de passe fort comme réponse, aussi complexe que celui de votre messagerie, si cela est possible.

- **Changez les mots de passe par défaut de vos programmes et appareils** R6 **:** les identifiants et les mots de passe par défaut peuvent certes vous faciliter l'accès à un service (connexion sans fil, vidéosurveillance, etc.), ou vous permettre de faire fonctionner plus rapidement un appareil (imprimante réseau, routeur, téléphone, etc.). Tout attaquant peut facilement découvrir les mots de passe par défaut d'un appareil ou d'un programme, cela en consultant le manuel d'utilisation, ou en visitant des forums sur Internet. Pour empêcher les fouineurs ou les personnes malintentionnées de s'introduire dans votre système, vous devez modifier au plus tôt mots de passe et identifiants par défaut, si cela s'avère possible, de tous les composants de votre système d'information.

- **Activez la double authentification pour accéder à votre compte utilisateur d'un programme ou service** R7 lorsque vous en avez la possibilité : la double authentification est une protection contre le vol des mots de passe. Elle permet d'empêcher une personne possédant votre mot de passe d'accéder à votre système ou à vos comptes. Lorsque quelqu'un essaye de se connecter à votre compte, cette mesure de sécurité permet de vérifier par deux (parfois trois) méthodes différentes qu'il s'agit bien de vous. Pour se connecter à un compte utilisant la double authentification il faut connaitre votre mot de passe et, par exemple, un code PIN à usage unique qui vous est envoyé par SMS.

Pour aller plus loin, les organisations possédant les compétences nécessaires (administrateur système et réseaux) doivent mettre en œuvre les recommandations[27] de la CNIL en matière de sécurisation de l'authentification par mot de passe, de conservation et de renouvellement des mots de passe dans leurs réseaux.

Cette fiche contient 7 recommandations.

Références :

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe
https://www.ssi.gouv.fr/guide/mot-de-passe/
https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires
https://www.cnil.fr/pourquoi-securiser-au-maximum-le-mot-de-passe-de-votre-boite-email
https://www.economie.gouv.fr/files/bro-guide-secu-info-print_0.pdf
https://support.microsoft.com/fr-fr/help/4027579/windows-10-create-a-password-reset-disk-for-a-local-account

27 https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

N°4

Fiche n°4

Messagerie électronique

Instrument essentiel de communication interne ou externe pour les organisations, la messagerie électronique est aujourd'hui la principale cible des attaquants, qui cherchent à dérober, corrompre ou détruire **des données**, le patrimoine de toute organisation. Bien des messages électroniques envoyés ou reçus par des collaborateurs de l'organisation sont sensibles (gestion de données personnelles, documents officiels, accès utilisateurs, etc.) et soumis aux différentes réglementations (RGPD, déclaration CNIL[28], etc.).

Les recommandations et les précautions suivantes sont essentielles pour protéger vos échanges électroniques, prévenir les attaques ou en diminuer les effets.

La messagerie électronique

- **Privilégiez les messageries qui garantissent le respect de la vie privée sur Internet** R1 **:** par exemple, la messagerie française Mailo ou les européennes MailFence, ProtonMail, Tutanota ou GMX. Préférez des sociétés françaises ou européennes plutôt que des géants étrangers qui analysent et archivent vos conversations.

- **Chiffrez les messages lorsque les données échangées sont à caractère personnel ou sensibles[29]** R2 **:** vous pouvez le faire par vous-même, les solutions gratuites existent (OpenPGP), mais leurs mise en œuvre nécessite de bonnes compétences en informatique. Vous pouvez aussi choisir une messagerie sécurisée intégrant un module de chiffrement des données. Ces messageries sont en général payantes, mais leur utilisation est simple, intuitive.

Le courrier électronique n'est pas un moyen de communication sécurisé pour échanger des données personnelles. Une simple erreur de manipulation peut provoquer la divulgation de données à des destinataires non autorisés. Afin de protéger les échanges, et notamment lorsque les informations échangées sont sensibles (données à caractère personnel, données financières, etc.), les organisations peuvent se tourner vers le service de coffre-fort numérique[30]. En outre, un coffre-fort numérique peut servir également d'espace de stockage sécurisé, ce qui n'est pas le cas de la messagerie électronique.

- **Evitez les messageries des fournisseurs d'accès à l'Internet** R3 **:** utilisez des messageries privées de préférences européennes. N'utilisez pas, par facilité, l'adresse offerte par votre fournisseur d'accès Internet (FAI), car celle-ci ne vous appartient pas, et si vous changez de prestataire vous perdrez cette adresse au bout de quelques mois.

28 La mise en place d'un dispositif de contrôle de la messagerie électronique par l'employeur doit être déclaré à la CNIL.
29 Voir la fiche « Gestion des données et RGPD ».
30 Voir la partie « Service coffre-fort numérique » de la fiche « Stockage des données ».

- **Paramétrez votre messagerie** R4 **:** les paramètres par défaut des messageries et des logiciels clients de messageries (Thunderbird, Outlook, etc.) sont souvent trop permissifs et contraires aux principes élémentaires de précaution. Vous pouvez vous référez au Guide pratique de paramétrage de la messagerie[31].

L'adresse électronique

- **Séparez les usages** R5 **:** utilisez une adresse pour l'usage professionnel et une autre pour l'usage privé. Idéalement, utilisez une adresse différente pour chaque nouveau service[32], avec des mots de passes toujours robustes et différents (voir la fiche 3 « Mots de passes »). Plus vous avez d'informations au même endroit, plus les effets d'une potentielle intrusion seront graves.

- **N'exposez pas votre adresse électronique sur l'Internet** R6 **:** vous risqueriez alors de recevoir des spams incessants. En effet, des robots (ordinateurs programmés pour réaliser des tâches automatiques) scrutent en permanence les sites Web afin de collecter les adresses des messageries électroniques qui s'y trouvent. Les bases de données ainsi constituées sont ensuite revendues à des tiers, régies publicitaires ou personnes malveillantes (spammeurs, pirates, etc.). Si vous êtes obligé d'exposer votre adresse électronique en ligne, dissimulez-la en remplaçant les caractères spéciaux, tel que « @ » et « . » respectivement par « (at) » et « (dot) », ou par n'importe quelle autre valeur; par exemple, adresse@exemple.com peut s'écrire de manière compréhensible pour les humains adresse(at)exemple(dot)com, elle pourra alors tromper certains robots.

- **Protégez les adresses électroniques de vos contacts** R7 **:** lorsque vous transférez un message, pensez à effacer les adresses qui y sont visibles (dans les champs destinataire (A) & copie (Cc)) et qui ne sont pas strictement nécessaires à la compréhension du message. Lors des diffusions massives de courriels informatifs mettez les adresses des destinataires en copie invisible (Cci), cela vous permettra de ne pas dévoiler vos listes de contacts.

La forme et le fond d'un courriel électronique

- **Regardez attentivement le nom et l'adresse de l'expéditeur du message que vous avez reçu, cela afin de bien vérifier que cette adresse est bien légitime** R8 **:** l'usurpation d'adresses électroniques est une forme de piratage très répandue, qui vise à tromper le destinataire d'un courriel en lui faisant croire que l'expéditeur est une organisation officielle ou l'une de ses connaissances. Vous pouvez également recevoir des messages qui semblent provenir de votre propre adresse électronique, le but étant ici d'attiser votre curiosité. Gardez à l'esprit que même un expéditeur de « confiance » peut aussi, à son insu (s'il a été piraté), vous demander une aide financière ou vous envoyer un message infecté.

31 https://www.cert.ssi.gouv.fr/information/CERTA-2000-INF-002/
32 Voir la partie « Les alias »

- **Vérifiez le ton, la formulation, la grammaire et l'orthographe employés dans tout courriel reçu** R9 **:** tout indice qui pourrait éveiller vos soupçons, vous mettre en garde quant à l'origine effective et la finalité réelle du message électronique, les incohérences de forme ou de fond, par exemple, un message en français dont l'objet est écrit en anglais ou dans une autre langue, des messages alarmistes ou qui attisent votre curiosité (« vous avez gagné, vous venez de toucher un héritage, cliquez sur ce lien, ouvrez la pièce jointes,... », etc.), des messages d'alertes de connexion à l'un de vos comptes en ligne (« votre compte a été piraté, merci de vérifier votre mot de passe sur ce lien,... », dans ce cas, contactez le service légitime concerné pour que celui-ci vous confirme/infirme l'alerte). **Ne répondez jamais à ce type de messages et ne les faites pas suivre à vos contacts.**

- **N'envoyez aucune information confidentielle par courriel électronique** R10 **:** l'hameçonnage (phishing en anglais) vise à obtenir du destinataire d'un courriel d'apparence légitime des informations, tels vos identifiants de connexion à des comptes en ligne, vos mots de passe, vos coordonnées bancaires, etc. Ces informations ne doivent jamais être demandées ni transiter via un courriel électronique. En cas de doute, contactez par téléphone le correspondant légitime afin qu'il vous confirme sa demande; signifiez lui alors que vous refusez d'envoyer de telles informations par messagerie électronique. Ne faites aucune action dans la précipitation.

- **Supprimez les pourriels (messages contenus dans vos spams), les messages douteux ou ceux contenant des identifiants et mots de passe** R11 **:** trier régulièrement vos courriels électroniques contribue à la mise en place d'une procédure de pré-archivage électronique[33].

Le contenu d'un courriel électronique

- **Analysez les pièces jointes** R12 **:** ne téléchargez jamais de pièce jointe reçue dans un courriel douteux (messages d'inconnus, demandes inhabituelles de vos collègues ou amis, etc.) ou dans un spam, car celles-ci pourraient être infectée. Vérifiez aussi l'extension de la pièce jointe reçue, si le fichier a une double extension, par exemple, nom_fichier.txt.exe, supprimez le message et le fichier au plus vite (voir le tutoriel « Afficher les extensions des fichiers »). Lorsque vous devez télécharger une pièce jointe, analysez-la avant de l'ouvrir à l'aide de votre antivirus en vous étant assuré que ce dernier est bien à jour.

Si vous êtes certain que la pièce jointe que vous avez reçue ne contient pas de données personnelles ou sensibles, vous pouvez l'analyser à l'aide d'un outil de multiscanning[34] en ligne, comme VirusTotal (voir le tutoriel « Analyser un fichier ou un lien avec VirusTotal »). En effet, les Conditions Générales de l'Utilisation (CGU) de ces services en ligne précisent généralement que tout fichier qui serait soumis à l'analyse deviendrait alors la propriété de l'entreprise qui fournit le service, ce qui compromet donc la confidentialité des fichiers analysées et limite fortement l'utilisation de tels outils.

33 Voir la fiche 10 « Archivage électronique ».
34 Des outils en ligne qui analysent vos fichiers et facilitent la détection rapide de logiciels malveillants à l'aide de plusieurs antivirus ou anti-logiciels malveillants.

- **Analysez les liens URL** R13 **:** avant de cliquer sur un lien, copiez-le et analysez-le à l'aide des outils de multiscanning en ligne (voire le tutoriel « Analyser un fichier ou un lien avec VirusTotal »).

- **Ne cliquez pas sur des liens de désinscriptions** R14 **:** au mieux, de tels liens servent à confirmer aux spammeurs que votre adresse électronique est réelle. Au pire, vous risquez d'infecter votre ordinateur. Ne vous désabonnez que des newsletters auxquelles vous savez que vous vous êtes réellement abonné (par exemple, une liste de diffusion d'un magasin). Dans ce cas, désabonnez-vous des newsletters indésirables dans les préférences de votre compte personnel en vous connectant directement au site légitime ou en informant l'administrateur du site.

- **Faites attention aux liens raccourcis** R15**,** par exemple de type http://bit.ly/Q4455Gpf6, ou http://goo.gl/48742JjvI45575, etc. Ce type de lien sert à dissimuler d'autres liens trop longs. Souvent utilisés par des réseaux sociaux, ces liens peuvent également vous rediriger vers un site malveillant. Il existe des outils en ligne permettant de démasquer le site de destination qui est caché derrière de tels liens[35].

- **Désactivez le téléchargement automatique des images** R16 **:** des liens URL peuvent se cacher derrière des images contenues dans des messages électroniques. Un clic accidentel peut alors vous rédiriger vers un site malveillant. En outre, des images peuvent être utilisées pour vous pister grâce à la technologie pixel espion. Il s'agit alors d'images de très petite taille, souvent invisibles et donc non repérables par l'utilisateur, qui permettent la génération de cookies tiers, utilisés, par exemple, par des **serveurs publicitaires** pour suivre votre **comportement**.

Les alias

Un alias est une adresse électronique secondaire que de nombreux logiciels de messagerie électronique vous autoriseront à créer. Cette adresse secondaire redirigera les messages qui lui sont envoyés vers votre compte de messagerie principal. Vous trouverez donc dans votre boîte de réception l'ensemble des messages provenant à la fois de votre compte de messagerie principal mais aussi des adresses alias. En fonction de votre opérateur de messagerie, vous avez la possibilité de créer un nombre déterminé d'alias, ces adresses alias pointeront toutes vers votre boîte de réception.

L'intérêt principal d'un alias est de créer des adresses supplémentaires qui servent à communiquer un identifiant différent à chacun de vos interlocuteurs, selon vos besoins et sans que vous ayez à changer de boîte de réception. Vous pourrez ainsi séparer les usages tout en protégeant votre véritable adresse électronique. Par exemple, si votre adresse principale est nom.prenom@votre-domaine.fr, vous pouvez créer des alias du type contact@votredomaine.fr ou nom_du_site_web@votredomaine.fr. Vous pouvez dédier l'une des adresses alias pour vous inscrire sur un site Web particulier, et une autre pour un autre.

35 https://unshorten.it

Toutes les réponses envoyées à ces deux adresses alias arriveront sur votre adresse de messagerie principale, vous verrez ainsi aisément quel sont les sites qui revendent votre adresse. Une adresse alias peut être supprimée à tout moment, par exemple lorsque vous recevez trop de messages inhabituels ou non souhaités (spams) sur l'une de ces adresses secondaires.

Pour aller plus loin et afin de sécuriser le trafic lié aux sites Web et à la messagerie électronique, les techniciens, les administrateurs ou les personnes chargées de la sécurité des systèmes d'information peuvent se référer au guide « Recommandations de sécurité relative à TLS » élaboré par l'ANSSI.[36]

Cette fiche contient 16 recommandations.

Références :

https://www.ssi.gouv.fr/particulier/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/
https://www.ssi.gouv.fr/administration/principales-menaces/lespionnage/
lattaque-par-hameconnage-cible-spearphishing/
https://www.cnil.fr/fr/le-controle-de-lutilisation-dinternet-et-de-la-messagerie-electronique
https://www.cert.ssi.gouv.fr/information/CERTA-2000-INF-002/
https://www.cert.ssi.gouv.fr/actualite/CERTFR-2015-ACT-052/
https://blog.provectio.fr/spam-comment-se-proteger-des-courriers-indesirables/
https://www.mediation-telecom.org/uploads/publications/Se%20prote%CC%81ger%20contre%20le%20phishing.pdf

36 https://www.ssi.gouv.fr/uploads/2017/07/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf

Fiche n°5

Applications

De nombreuses applications n'ont pas été conçues pour être sécurisée par défaut, mais pour rendre un service informatique. Tout programme est susceptible de présenter des vulnérabilités exploitables, plus vous téléchargez et installez de logiciels sur votre ordinateur, plus vous augmentez potentiellement la surface d'attaque. En outre, les applications peuvent collecter et transmettre des informations potentiellement sensibles du système (géolocalisation, carnet d'adresse, documents, etc.), ainsi que vos données. Limitez votre exposition aux cyber-menaces en suivants les recommandations suivantes :

- **Téléchargez chaque logiciel sur le site officiel de son éditeur** R1 **:** ne téléchargez jamais de logiciel sur d'autres sites que celui de l'éditeur. Vous pouvez également vous référer à la liste des logiciels libres fournie par le Socle Interministériel de Logiciels Libres[37].

- **Avant d'exécuter un logiciel téléchargé sur Internet, analysez-le à l'aide de votre logiciel anti-virus** R2 **:** il existe également des outils de multiscanning[38] en ligne, comme VirusTotal (voir le tutoriel « Analyser un fichier ou un lien avec VirusTotal »), qui permettent d'analyser les exécutables et divers fichiers téléchargés sur Internet à l'aide de nombreux antivirus. S'il s'avère que le logiciel ou le fichier analysé est infecté, surtout ne l'exécutez pas et détruisez-le immédiatement.

- **Mettez à jour tous les logiciels installés sur votre ordinateur** R3 **:** tout comme votre système d'exploitation, les logiciels qui sont installés sur votre ordinateur doivent être régulièrement mis à jour. Si cela est possible, configurez les logiciels pour que les **mises à jour de sécurité se fassent de manière automatique.**

- **Désinstallez les logiciels non essentiels à votre travail** R4 **:** bien souvent il vous est proposé avec votre systèmes d'exploitation des logiciels dont vous n'avez pas besoin pour votre usage professionnel, il faut désinstaller ces applications qui vous sont inutiles. Par exemple, le système Windows est fourni avec un grand nombre d'applications préinstallées. Il s'agit des applications universelles (news, sport, météo, jeux, cuisine, Skype, santé et fitness, Booking, etc.) ou les programmes classiques de bureau (souvent des versions d'essai de logiciels payants, parfois des harceliciels). Ces logiciels ralentissent inutilement votre travail et votre système, peuvent comporter des failles de sécurité et représenter un risque pour votre système et vos données (voir le tutoriel « Désinstaller les applications »). N'installez pas un logiciel lorsque vous n'en avez pas l'usage.

Certaines applications universelles ne peuvent pas être désinstallées (Microsoft Edge, Cortana, etc.), dans ce cas, il est recommandé de mettre en œuvre des règles de restriction à l'aide d'un logiciel de contrôle des applications, par exemple AppLocker sous Windows ou AppArmor sous Linux. Cependant,

37 https://sill.etalab.gouv.fr/fr/software
38 Des outils qui exécutent plusieurs anti-logiciels malveillants ou antivirus simultanément.

l'utilisation de ce type de logiciel nécessite d'avoir de bonnes compétences en informatique. Pour Windows, nous vous recommandons de vous référer au Guide de l'ANSSI, « Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows[39] ».

- **Limitez les accès octroyés aux logiciels installés** R5 **:** les applications peuvent accéder à des ressources potentiellement sensibles de votre système, comme la géolocalisation, la caméra, le microphone, les carnets d'adresse, etc. Bloquez l'accès à ces ressources pour des applications installées sur votre système (voir le tutoriel « Restreindre les autorisations accordées aux applications »).

- **Paramétrez vos logiciels** R6 **:** les paramétrages par défaut sont souvent trop permissifs (pièces jointes chargées automatiquement ou liens qui s'ouvrent à l'ouverture du courriel, utilisation de *Cloud*, des macros, etc.) et vont à l'encontre des principes élémentaires de précaution. Par exemple, désactiver la collecte et l'envoie d'informations aux éditeurs des logiciels, bloquer l'accès aux ressources de votre ordinateur (microphone, caméra) sont les précautions de base à effectuer.

- **Utilisez un moteur de recherche qui respecte la confidentialité de vos recherches en ligne** R7 **:** par exemple, un moteur ou un métamoteur[40] français, tel que Qwant ou Lilo. Évitez les moteurs de recherche étrangers, surtout ceux qui collectent, analysent et stockent vos données personnelles.

En règle générale, n'utilisez que des programmes d'éditeurs connus, et uniquement ceux qui vous sont nécessaires. Face à un programme peu répandu dont vous avez besoin pour votre travail, ou au site d'un éditeur peu connu, renseignez-vous avant de le télécharger et de l'installer, consultez les avis des internautes grâce à votre moteur de recherche, et passez le fichier exécutable à VirusTotal avant de l'installer.

Cette fiche contient 7 recommandations.

Références :

https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
https://www.ssi.gouv.fr/uploads/2017/01/np_securisation_windows10_collecte_de_donnees_v1.2.pdf
https://www.cnil.fr/fr/securite-securiser-les-postes-de-travail
https://www.cnil.fr/fr/reseaux-sociaux-limiter-lacces-des-applications-tierces-vos-donnees
https://www.cert.ssi.gouv.fr/information/CERTA-2006-INF-006/

39 https://www.ssi.gouv.fr/uploads/2013/12/np_applocker_notetech-v2.pdf
40 Un métamoteur envoie les requêtes à plusieurs moteurs de recherche et retourne les résultats de chacun d'eux.

Fiche n°6

Supports amovibles

Les médias et supports de stockage amovibles (clé USB, carte SD, disque dur externe, etc.) sont largement utilisés par les agents pour stocker, transporter et partager des données. Cependant, l'utilisation incontrôlée de ces supports certes très pratiques et en apparence inoffensifs peut accroître le risque de diffusion de logiciels malveillants et donc accélérer les effets d'une cyber-attaque.

Les recommandations suivantes vous permettront de réduire les risques associés à l'utilisation des supports amovibles :

- **Analysez à l'aide de votre logiciel anti-virus tout support que vous connectez à votre ordinateur via un port périphérique (tel qu'un port USB) R1.**

- **Désactiver l'exécution automatique des médias et périphériques R2 :** un programme malveillant peut s'exécuter à partir d'un support amovible dès que celui-ci est connecté à votre ordinateur. Désactiver l'exécution automatique est une bonne pratique qui permet d'empêcher l'exécution de programmes de manière automatique lors de la connexion d'une clé USB ou d'un disque dur externe (voir le tutoriel « Désactiver l'exécution automatique à partir des supports amovibles »).

- **Évitez de connecter des supports sur des comptes administrateurs R3 :** les programmes stockés, par exemple, sur une clé USB, héritent automatiquement des droits utilisateur de la session sur laquelle la clé est connectée (voir la fiche 2 « Sécurité du poste de travail »). La connexion d'un support amovible sur une session administrateur ne doit se faire que si cela est indispensable à la maintenance du système.

- **Séparez les usages R4** : ne stockez pas vos données personnelles et professionnelles sur le même support. Ne connectez pas à des postes reliés au réseau de l'organisation des équipements et des supports amovibles personnels (clés USB, disques durs externes, lecteurs MP3/MP4, téléphones, tablettes, etc.).

- **Achetez des supports amovibles neufs et scellés R5 :** ne les achetez pas dans des dépôts ventes. Évitez les clés et les disques trop bon marché sur des sites de vente en ligne hébergés à l'étranger, les clés offertes lors de salons, de conférences ou de colloques, et cela même si la tentation de se les approprier est forte (amusantes ou jolies). En effet, des personnes malveillantes peuvent infecter ces produits en libre-service faciles à emporter.

- **Ne connectez jamais à votre ordinateur les supports trouvés ou proposés par des personnes de passage R6 :** cela, quel que soit le prétexte, par exemple, une personne peut vous demander de l'aide pour recharger quelques minutes son téléphone ou son lecteur MP3, ainsi sera-t-elle en mesure de dérober toutes les données contenues sur votre ordinateur ou d'y installer à votre insu un logiciel espion. Pour éviter de brancher par réflexe

un support qu'on vous tend, vous pouvez utiliser des verrous de ports USB, ceux-ci vous rappelleront que brancher un appareil sur votre ordinateur n'est jamais un acte anodin.

Les organisations peuvent renforcer leur politique de gestion des supports amovibles en obligeant tous les personnels à passer tout support externe au crible d'une station blanche. Il s'agit d'une machine séparée du réseau qui analyse les médias amovibles à l'aide de logiciels anti-virus. Le CIRC du Luxembourg (The Computer Incident Response Center) offre une méthodologie simple pour fabriquer à moindre frais une station blanche à partir d'un Raspberry Pi[41]. Afin de bien définir quelles sont les fonctions de sécurité attendues et les exigences associées à ce type de produit, l'ANSSI a élaboré un guide auquel vous pouvez vous référer « Profil de fonctionnalités et de sécurité – sas et station blanche »[42].

- **Protégez et formatez vos supports de stockage amovibles** R7 **:** les supports amovibles peuvent facilement être perdus, endommagés, empruntés ou volés. L'organisation et les collaborateurs peuvent être soumis à des sanctions pénales et financières si des données sensibles ou à caractère personnel (voir la fiche 1 « Gestion des données et RGPD ») sont perdues ou compromises. En outre, la perte de données peut entraîner une atteinte importante à la réputation de l'organisation en érodant la confiance des citoyens. Évitez donc de stocker vos supports à proximité de sources d'eau ou de chaleur, dans des endroits où ils peuvent subir des chocs, où vous pourriez les perdre, où ils pourraient être intervertis avec des supports similaires, vides ou corrompus, ou être volés. Ne jetez jamais vos supports endommagés, faites-les détruire physiquement (faites appel à des sociétés spécialisées qui vous délivreront des certificats attestant que les données de l'organisation ont bien été détruites. Ces entreprises assurent la destruction en petits copeaux et le recyclage écologique de vos supports informatiques), et assurez-vous de la destruction de leurs contenus. En outre, lorsque vous utilisez un support amovible pour partager des documents, n'oubliez jamais de le formater après utilisation.

- **Chiffrez les supports contenant les données sensibles ou à caractère personnel** R8, malgré toutes nos recommandations vous ne serez pas à l'abris d'une perte, d'un vol ou d'un piratage de vos matériels. Toutefois, si vos supports sont chiffrés, dans la plupart des cas le voleur ne cherchera pas à les décrypter, car cela lui prendrait trop de temps pour un résultat de surcroit incertain (voir le tutoriel « Mettre en place un conteneur chiffré VeraCrypt »).

Cette fiche contient 8 recommandations.

Références :

https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
https://www.cert.ssi.gouv.fr/information/CERTA-2006-INF-006/
https://sisse.entreprises.gouv.fr/fr/utiliser-des-supports-amovibles-de-facon-securisee

41 https://www.circl.lu/projects/CIRCLean/
42 https://www.ssi.gouv.fr/uploads/2020/08/anssi-profil_de_fonctionnalites_et_de_securite-sas_et_station_blanche_reseaux_non_classifies-v1.0.pdf

Fiche n°7

Appareils nomades

Le développement du télétravail et l'utilisation des appareils nomades (smartphone, tablette, ordinateur portable) est en pleine croissance dans toutes les organisations publiques et privées. Cependant, ces pratiques exposent le système d'information de l'organisation à de nouveaux risques, la gestion des accès distants au réseau interne, l'utilisation parfois des appareils nomades personnels dans un contexte professionnel (AVEC en français pour « apportez votre équipement personnel de communication » ou BYOD[43] en anglais), pratique que nous conseillons de bannir.

Les recommandations suivantes permettront de faire face à ces enjeux et de sensibiliser l'ensemble des acteurs du nomadisme :

- **Respectez les recommandations élémentaires de sécurité** R1 **:** les recommandations issues des fiches précédentes, 2 « Poste de travail », 3 « Mots de passe », 4 « Messagerie électronique » et 5 « Applications », sont applicables dans le cadre d'utilisation des appareils nomades :
  - Installez un logiciel anti-virus ;
  - Appliquez les mises à jour de sécurité du système et des applications installées ;
  - N'installez que des applications officielles et nécessaires ;
  - Limitez les autorisations et les accès accordées aux applications : la plupart des applications n'ont pas besoin d'accéder à votre carnet de contact ou à votre géolocalisation pour bien fonctionner ;
  - Désactivez les services de connexion lorsque vous ne les utilisez pas (Bluetooth, Wi-Fi, 3G, 4G, etc.) et évitez les connexions aux réseaux publics ou inconnus ;
  - Activez le verrouillage automatique de vos appareils ;
  - Activez le chiffrement des données stockées sur vos appareils nomades et sur les cartes d'extension mémoire si vous les utilisez ;
  - Faites des sauvegardes ou des synchronisations régulières.

- **Séparez les usages** R2 **:** n'utilisez pas des appareils nomades personnels à des fins professionnelles, car l'utilisation d'appareils non maitrisés par la collectivité expose considérablement son réseau aux risques de sécurité. Avec les BYOD, la distinction entre les données privées et professionnelles devient de surcroit impossible, ce qui augmente également les risques juridiques. En effet, d'après la CNIL « l'employeur est responsable de la sécurité des données personnelles de son organisation, y compris lorsqu'elles sont stockées sur des terminaux dont il n'a pas la maitrise physique ou juridique ».

43 bring your own device

- **Sécurisez les accès distants aux ressources** R3 **:** lorsque les collaborateurs se déplacent ou ont recours au télétravail, tous les accès aux ressources de l'organisation (données, applications métiers, serveurs) doivent être maitrisés et sécurisés. Seules les connexions utilisant un VPN[44] (Virtual Private Network) ou de personnes utilisant les appareils sécurisés et administrables doivent être autorisées. Les accès distants doivent être contrôlé par un dispositif d'authentification de l'utilisateur (si possible robuste, tel un certificat électronique, etc.) et strictement filtrés à l'aide d'un pare-feu.

- **Utilisez les codes secrets pour déverrouiller vos appareils** R4 **:** en plus du code PIN de la carte SIM, mettez en place un système pour déverrouiller vos appareils (code, mot de passe, schéma, empreinte, etc.). Préférez les codes à 6 chiffres et évitez les codes trop simples, comme 0000 ou 1234 (codes originels de nombreuses cartes SIM ou d'interrogation de votre répondeur).

- **Prévoyez une procédure en cas de perte ou de vol d'un appareil nomade** R5 **:** telles que le verrouillage des dispositifs à distance, l'effacement des données, l'effacement des mots de passe :
  - Nous vous recommandons de conserver le code IMEI des appareils mobiles : il s'agit d'un numéro de 15 à 17 chiffres permettant d'identifier de manière unique un appareil mobile. Pour le connaître, il suffit de taper *#06# sur le clavier de votre appareil. Ce code est également noté sur sa boîte d'emballage et sur la facture d'achat. En cas de perte ou de vol, ce code peut permettre de bloquer l'usage de l'appareil sur tous les réseaux ;
  - Certains appareils possèdent le système d'effacement automatique lorsqu'un code est erroné est tapé à de trop nombreuses reprises ;
  - L'organisation peut aussi mettre en œuvre un logiciel de gestion des appareils mobiles (MDM) qui permet de superviser le parc d'appareils nomades, qu'il s'agisse de tablettes, de téléphones ou d'ordinateurs portables ;
  - Assurez vos appareils nomades : privilégiez des assurances qui offrent des couvertures tous risques (perte, vol, casse, oxydation) et toutes causes.

- **Sensibilisez les agents aux risques spécifiques liés à l'utilisation d'appareils nomades** R6 **:** tels que le vol, la perte de l'appareil, l'utilisation de réseaux Wi-Fi publics non sécurisés, etc. Définissez une charte claire qui précise les responsabilités de chacun (vous trouverez un modèle en annexe), ainsi que les précautions à prendre en cas d'un incident lié à l'utilisation d'un appareil nomade.

Faites attention lorsque vous scannez un code QR[45] avec votre appareil mobile. D'apparence innocente, ces codes barre en forme de petits carrés sont de plus en plus omniprésents. Le simple fait de les scanner ou les prendre en photo permet de réaliser de nombreuses actions, comme visiter un site Internet, se connecter à une borne Wi-Fi, déclencher un appel, faire un payement, installer une application, etc. Ces codes QR utiles pour les simples utilisateurs peuvent être facilement falsifiés et exploités par des personnes malveillantes.

44 Un réseau privé virtuel qui permet des échanges de données sécurisés entre un poste de travail distant et le réseau interne de l'organisation.

45 Le code QR est un type de code-barres constitué de modules noirs disposés dans un carré à fond blanc. L'agencement de ces points définit l'information que contient le code.

- **Installez un lecteur de code QR sécurisé** R7 **:** ces dispositifs gratuits vérifient les URL cibles à la recherche de codes malveillants, ce qui vous permet de scanner ces codes en toute sécurité (Kaspersky QR Scanner, Sophos Mobile Security, ...).

Pour aller plus loin, vous pouvez vous appuyer sur les guides de l'ANSSI « Recommandations sur le nomadisme numérique »[46] et « Passeport de conseils aux voyageurs »[47].

Cette fiche contient 7 recommandations.

Références :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/appareils-mobiles
https://www.cnil.fr/en/node/15760

46 https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf
47 https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf

N°8

Fiche n°8

Stockage des données

Les organisations sont tenues à l'obligation légale d'assurer la sécurité des données qu'elles détiennent. Sécuriser les moyens de stockage des données qu'elles utilisent, qu'ils soient internes ou externes, permet de minimiser le risque de perte ou de vol, de divulgation non autorisée, de corruption ou encore d'une destruction accidentelle des données. C'est un domaine qui revêt une importance cruciale pour les organisations car la majorité des violations de données sont causées par une défaillance de la sécurité de ces stockages.

Stockage en interne

Un serveur local de stockage de données en réseau, appelé Network Attached Storage (NAS), permet de stocker et de partager des données avec d'autres ordinateurs de votre réseau local. Un NAS est pourvu d'un système de refroidissement, d'un processeur, de mémoire vive et d'un système de gestion des données. Ainsi un NAS est plus robuste et performant qu'un simple disque dur externe. Les serveurs NAS sont faciles d'utilisation et leur mise en œuvre reste relativement simple. Toutefois, il faut savoir que cet équipement peut être vulnérable. Un ordinateur infecté par un rançongiciel qui se connecte à votre réseau peut, par exemple, infecter le serveur et corrompre toutes les données qui y sont stockées. De plus, ce type d'équipement offre de nombreux services réseau supplémentaires (serveur de messagerie, serveur DHCP, VPN, etc.), ce qui augmente considérablement sa vulnérabilité.

En complément des recommandations données dans la fiche 11 « Serveurs et locaux », voici quelques conseils relatifs aux serveurs de stockage :

- **Bien cerner les besoins de l'organisation** R1 **:** les prix des serveurs NAS sont variables et les possibilités offertes d'un modèle à l'autre sont différentes. Avant d'investir dans un serveur de stockage, documentez-vous sur les capacités des modèles du marché.

- **Évitez la technologie RAID 0**[48] R2 **:** le RAID (*Redundant Arrays of Inexpensive Disks*) est un ensemble de techniques de stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer les performances, la sécurité ou la tolérance aux pannes du système. La technologie appelé RAID 0 n'offre aucune tolérance aux pannes : une défaillance du disque dur remettrait en cause l'intégrité des données qui y sont stockées. Choisissez les technologies telles que RAID 1 ou RAID 5.

- **Faites des sauvegardes régulières** R3 **:** toutes les données stockées sur un serveur NAS doivent être sauvegardées sur un support externe pouvant être déconnecté et qui ne sera pas stocké au même endroit que le NAS (voir la fiche 9 « Plan et stratégies de sauvegarde »).

48 Deux disques durs, ou plus, en parallèle, la perte d'une seule unité de stockage entraînant alors la perte de toutes les données du volume RAID. Nous parlons ici de RAID matériel. Il existe aussi des solutions logicielles pour faire du RAID qui sont souvent moins coûteuses, mais qui sollicitent le processeur de votre machine.

- **Activez le chiffrement des données stockées** R4 **:** le chiffrement protège les données contre les accès non autorisés, à condition que la clé de déchiffrement/mot de passe soit stockés en lieu sûr (voir la fiche 3 « Mots de passe »).

Stockage en externe

L'informatique en nuage (*Cloud*) permet d'externaliser, c'est à dire de stocker et traiter les données sur des serveurs qui sont situés à distance des outils de travail. Il peut s'agir des logiciels supports, comme la messagerie électronique, les agendas, les outils de sauvegarde, ou les applications métiers. Le *Cloud* est une solution qui possèdent des avantages pratiques : données accessibles en ligne, ce qui facilite le travail en déplacement ou à distance, absence de certaines contraintes techniques, telle la maintenance de serveurs internes. Toutefois, le recours au *Cloud* peut générer de nombreux risques liés à la sécurité et la protection des données. En complément des recommandations que vous trouverez dans la fiche 12 « Externalisation », les éléments suivants nécessitent une étude approfondie :

- **L'infrastructure télécom interne** R5 **:** pour accéder aux données stockées en ligne un accès à Internet est indispensable. Il est nécessaire d'évaluer certains paramètres du réseau interne, telle la connectivité ou le débit Internet, car les investissements ou la mise à niveau peuvent être cher.

- **La localisation des données hébergées, l'emplacement des infrastructures informatiques et le pays d'origine du fournisseur du service** R6 **:** en fonction de la sensibilité des applications concernées, trois cercles de sécurité ont été définis dans la stratégie *Cloud* de l'État (circulaire no 6049-SG du 8 novembre 2018) :
  - Les données et applications les plus sensibles devront être hébergées dans un service *Cloud* interne français, totalement maîtrisé par l'État, disponible depuis un portail interministériel ;
  - Les données et applications de sensibilité moindre pourront être confiées à des hébergeurs français dans un *Cloud* dédié ;
  - Les données et applications peu sensibles pourront être hébergées par des acteurs français ou étrangers dans un *Cloud* externe accessible sur l'Internet. Un catalogue de ces offres porté par les centrales d'achat est prévu pour l'année 2021.

- **Les clauses du contrat** R7 **:** renoncez à l'utilisation des services *Cloud* qui proposent des contrats standard dont vous ne maitrisez pas les clauses. Sans en être conscientes, la plupart des organisations utilisent au quotidien des solutions *Cloud* dont les conditions générales d'utilisations sont évasives, non accessibles ou abusives. Ces outils, certes très attractifs en termes de facilité d'utilisation, sont proposés, voire imposés par votre système d'exploitation ou votre messagerie électronique, par exemple les logiciels de stockage et de partage de fichiers Dropbox, OneDrive ou Google Drive, la

messagerie Gmail, l'enregistrement automatique de vos documents par suite bureautique Microsoft Office 365 (voir le tutoriel « Désactiver OneDrive et supprimer les documents stockés en ligne »). Avant signature du contrat, il est nécessaire de définir des clauses contractuelles propres, qui répondent aux besoins de l'organisation en matière de la sécurité technique et juridique des données.

Le service de coffre-fort numérique. Plus qu'un simple outil de stockage de données en ligne, un coffre-fort numérique est un système sécurisé de conservation de données à valeur probante qui permet de recevoir, stocker ou partager les données dans des conditions permettant de justifier de leur intégrité et l'exactitude de leur origine. Un service de coffre-fort numérique peut être utilisé de manière très différente d'une structure à l'autre : conservation de documents, réalisation de démarches administratives avec partage de pièces justificatives, récupération ou dépôt de documents déposés par un partenaire ou prestataire, etc.

Le cadre législatif du service de coffre-fort numérique est riche et précis[49]. Les contraintes organisationnelles et techniques imposées par la Loi obligent donc les fournisseurs de service à concevoir des infrastructures complexes, c'est pourquoi les organisations doivent **s'assurer de la conformité du fournisseur de service à ces exigences** R8. Nous recommandons aux organisations de choisir des fournisseurs qui ont bénéficié d'une certification de conformité à un cahier des charges établi par l'ANSSI. Les normes AFNOR relatives aux systèmes d'archivage électronique[50] peuvent également être appliquées aux services de coffre-fort numérique. En outre, lorsque les données collectées et stockées dans un coffre-fort numérique sont à caractère personnel, le service proposé devra être en règle avec le Règlement général sur la protection des données (RGPD).

Attention, il ne faut pas confondre un service de coffre-fort numérique (comme Digiposte, Coffreo, etc.) avec une messagerie électronique sécurisée, un fichier chiffré, un gestionnaire de mot de passe, de type KeePass, appelé aussi parfois coffre-fort des mots de passe, ou encore un composant coffre-fort numérique d'un système d'archivage électronique (voir la fiche 10 « Archivage électronique »).

Cette fiche contient 8 recommandations.

Références :

https://www.cert.ssi.gouv.fr/actualite/CERTFR-2016-ACT-021/
https://solidarites-sante.gouv.fr/IMG/pdf/vademecum_coffre-fort-numerique.pdf
https://www.legifrance.gouv.fr/eli/decret/2018/5/30/ECOI1801826D/jo/texte/fr
https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=A6647FDC29F61AC42CAE113859E1810D.tpdila08v_2?idArticle=JORFARTI000033202902&cidTexte=JORFTEXT000033202746&dateTexte=29990101&categorieLien=id
https://blog.outscale.com/fr/enjeux-et-perspectives-du-cloud-pour-le-secteur-public

49 art. 87 de la Loi pour une République numérique, art. L103 du Code des postes et des communications électroniques, décret n° 2018-418 du 30 mai 2018, etc.
50 Voir la fiche 10 « Archivage électronique »

Fiche n°9

Plan et stratégies de sauvegarde

La finalité d'une sauvegarde est de restaurer les données lorsqu'elles ont été endommagées ou détruites, soit par des erreurs des utilisateurs, soit à cause de logiciels malveillants, tels les rançongiciels[51]. Elles constituent également un atout important pour initier dans les meilleurs délais un plan de continuité ou de reprise d'activité informatique, au cas où une catastrophe venait à frapper votre système d'information, par exemple une panne suivie d'une défaillance matérielle ou logicielle, des conditions météorologiques extrêmes, etc.

Avant même de choisir les supports ou les solutions de sauvegarde, l'organisation doit **établir un plan de sauvegarde** R1**.** Ce plan doit être mis à jour à chaque déploiement d'un nouveau composant du système d'information de l'organisation (installation d'un serveur ou d'un poste de travail, achat d'un logiciel, etc.) et il doit définir au moins les points suivants :

- **Le périmètre des sauvegardes :** la liste des données à sauvegarder, les serveurs concernés, les postes de travail, les appareils mobiles, mais aussi les logiciels indispensables à l'exploitation des données, les systèmes d'exploitation, les prologiciels ou logiciels métiers : finances, RH, état civil, etc.

- **Le type des sauvegardes :** définissez les types de sauvegardes (complète, instantanée[52], synchronisation, etc.) appropriés aux types de données à sauvegarder (donnée froide[53] ou chaude[54]). Toutes les sauvegardes doivent être réalisées à l'aide de logiciels spécialisés (Bareos, Historique de fichiers de Windows, etc.). Une simple action consistant à copier-coller les données ou à copier un disque dur interne sur un disque dur externe ne peut pas être considérée comme une sauvegarde[55].

- **La fréquence et la planification des sauvegardes :** effectuez des sauvegardes à des intervalles réguliers et fréquents (sauvegarde journalière ou hebdomadaire). Leurs planifications doivent varier en fonction du type de sauvegarde ou d'environnement à sauvegarder. Par exemple, une sauvegarde complète, qui consiste à copier toutes les données d'un système, nécessite des ressources importantes (bande passante, mémoire vive, etc.). Par conséquent, elle peut être planifiée à des heures creuses. Si l'organisation héberge un site Web qui utilise divers fichiers, des bases de données ou de applications métiers, il faut aussi penser à sauvegarder ces éléments aux mêmes horaires, car une incohérence dans des sauvegardes d'applicatifs risque de rendre inexploitable le système restauré.

- **La procédure d'exécution des sauvegardes et la restriction des accès :** seuls les agents habilités peuvent avoir accès aux sauvegardes et aux supports qui les hébergent. Ces accès doivent correspondre à un besoin réel,

51 https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
52 Une sauvegarde de l'état d'un système à un instant donné.
53 Les données qui sont rarement consultées.
54 Les données qui doivent être immédiatement accessibles, car souvent consultées.
55 Risque de conservation d'anciens fichiers/dossiers supprimés toujours présents dans la sauvegarde, qui prend de plus en plus de place, souci de restauration de codes sources de programme et/ou d'un site web, nombre de lectures/écriture limité pour les supports SSD, risque de se tromper entre un dossier et un raccourci du dossier, etc.

et être en lien avec l'exercice de leurs missions. En outre, les sauvegardes doivent être réalisées même lors des absences ou des congés des agents qui s'en occupent habituellement.

- **Les procédures et test de restauration :** il est indispensable de s'assurer de la copie effective, intégrale et fiable des données, ainsi que de tester leur restauration. Ce test doit être réalisé au moins une fois par an. Une trace technique des résultats de restauration doit être conservée.

- **La destruction des supports ayant contenu les sauvegardes :** ne jetez jamais les supports endommagés, détruisez-les, assurez-vous de la destruction de leurs contenus (la destruction physique pour les supports amovibles, la démagnétisation pour les bandes magnétiques).

Quelques soit les périmètres, les types ou les fréquences des sauvegardes définies dans le plan, les organisations peuvent s'appuyer sur la **stratégie de sauvegarde**, appelée « 3-2-1 »[56], basée sur les principes suivants :

→ Réaliser 3 copies de données[57] au moins ;

→ Sur 2 supports différents hébergés en interne ;

→ Et sur 1 site externe (cela peut être un *Cloud* sécurisé sur lequel vos données sont stockées chiffrées).

Au besoin, la stratégie de sauvegarde « 3-2-1 » peut être adaptée. Par exemple, lorsque la sauvegarde externe n'est pas possible/envisageable pour l'organisation, vous pouvez mettre la stratégie « 3-3 », qui consisterait à faire 3 copies au moins sur 3 supports différents hébergés en interne. Mais attention de ne pas garder tous les supports de sauvegarde au même endroit.

Dans tous les cas, **au moins l'un des supports de sauvegarde doit être amovible** R2, par exemple un disque dur externe, ou une bande magnétique. En effet, un serveur destiné à héberger les sauvegardes est en permanence connecté au réseau interne de l'organisation ce qui le rend vulnérable aux attaques par rançongiciel. Le bon usage de supports amovibles permet de protéger les sauvegardes d'une infection et de conserver les données critiques à la reprise d'activité.

Recommandations à suivre afin de sécuriser les supports de sauvegarde amovibles :

- **Préférez un disque dur externe à une clé USB** R3 **:** une clé USB peut être plus facilement perdue, endommagée ou volée.

- **Le support de sauvegarde doit être dédié** R4 **:** c'est-à-dire réservé exclusivement à la tâche « sauvegarde ».

56 https://www.economie.gouv.fr/files/170922_politiques-sauvegardes_v1.1.pdf
57 Une copie principale et deux sauvegardes.

- **Pensez à la capacité de stockage du support** R5 **:** celle-ci doit être supérieure à la capacité de stockage du système à sauvegarder.

- **Chiffrez le support contenant les sauvegardes** R6 **:** le chiffrement protège les sauvegardes contre les accès non autorisés. Conservez le mot de passe/la clé de déchiffrement en lieu sûr (voir la fiche 3 « Mots de passe »).

- **Protégez les supports contenant les sauvegardes** R7 **:** identifiez et étiquetez chaque support amovible de sauvegarde. Stockez-les dans un espace protégé contre les menaces physiques et environnementales (vols, chocs, incendies, dégâts des eaux, perturbations magnétiques, etc.) et physiquement éloigné des composants du système sauvegardé.

- **Déconnectez le support dès que la sauvegarde est terminée** R8 **:** afin de le protéger contre une éventuelle attaque.

Pour appliquer certains de ces conseils, vous pouvez vous appuyer sur des tutoriels suivants : « Sauvegarder les fichiers », « Restaurer les fichiers », « Sauvegarder Windows 10 à l'aide d'une image système », « Restaurer Windows 10 à partir d'une image système », « Mettre en place un conteneur chiffré VeraCrypt ».

Sauvegarde en externe

En l'absence des compétences nécessaires en informatique, les organisations peuvent confier une partie ou toute la gestion de la sauvegarde de leurs données à un prestataire externe. Toutefois, avant de confier leurs données à un prestataire, il leur est indispensable de **mener une analyse de risque, et, le cas échéant, une analyse d'impact relative à la protection des données** R9 (voir la fiche 1 « Données personnelles et RGPD »), qui portera sur la qualité des moyens de transmission et sur la sensibilité des données transmises.

Enfin, les données et les sauvegardes que l'organisation détient sont soumises à plusieurs régimes juridiques qui engagent sa responsabilité civile ou pénale. En amont de la signature d'un contrat d'infogérance, **l'organisation doit s'assurer que le contrat comprenne bien des clauses qui l'assurent de la confidentialité, de l'intégrité et de la disponibilité des données** R10 (voir la fiche 12 « Externalisation »).

Cette fiche contient 10 recommandations.

Références :

https://www.cnil.fr/fr/securite-sauvegarder-et-prevoir-la-continuite-dactivite
https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
https://www.economie.gouv.fr/files/170922_politiques-sauvegardes_v1.1.pdf
https://cyberveille-sante.gouv.fr/sites/default/files/documents/plan-ssi/Plan%20d%27action%20SSI%20-%20Fiche%20n%C2%B07%20-%20%20Sauvegardes%20r%C3%A9guli%C3%A8rement%20test%C3%A9es.pdf

Fiche n°10

Archivage électronique dans les collectivités territoriales

Tous les documents produits ou reçus dans un format électronique par une collectivité dans le cadre de son activité constituent une archive publique électronique. C'est le cas de la production bureautique et collaborative, des messageries électroniques, des fichiers image, son ou audiovisuel, des données issues des applications métiers, des projets de dématérialisation, etc.

réation ou la réception d'un document électronique, il entre dans l'âge des **archives courantes**. Lorsque le document n'est plus fréquemment usité mais que le service qui l'a produit peut encore en avoir besoin, le document entre dans l'âge des **archives intermédiaires**. Ces deux âges forment la **durée d'utilité administrative (DUA)**, durant laquelle les archives sont sous la responsabilité du service qui les a produites. Enfin, les documents dont la durée d'utilité administrative est échue constituent des **archives définitives**. Elles sont par conséquent conservées sans limitation de durée en vertu de leur valeur historique et patrimoniale.

Les articles L211-1 et L212-6 du code du Patrimoine affirment l'obligation pour les collectivités de se doter des moyens nécessaires à la bonne conservation de leurs archives électroniques. C'est le respect d'un cahier des charges précis, qui assurera **l'intégrité**, la **pérennité**, la **sécurité**, la **confidentialité** et la **traçabilité** des données, et qui permettra alors de donner aux archives électroniques une valeur probatoire, au même titre que pour des archives papier. La collectivité devra donc **mettre en place ce dispositif encadré par la Loi** R1.

Il ne faut pas confondre stockage, sauvegarde et archivage électronique. Si le stockage correspond simplement à un espace où l'on peut conserver des données, la sauvegarde se préoccupe de la continuité de fonctionnement des systèmes et des services informatiques. Enfin, l'archivage électronique sert à conserver des données à très long terme, tout en garantissant aux données les propriétés citées dans le paragraphe précédent, le stockage et la sauvegarde ne répondant pas à ces exigences.

Si le maire (ou le président de l'EPCI) est personnellement responsable de la bonne conservation des archives de sa commune ou de son établissement, chaque agent de la fonction publique est responsable des documents qu'il produit. Il est donc nécessaire de mettre en place des procédures auxquelles tous les agents d'une collectivité devront se soumettre :

- **Trier régulièrement les dossiers et classer les documents** R2 **:** chaque agent doit identifier correctement et lisiblement ses dossiers pour faciliter les futures opérations d'archivage et de recherche, la collectivité doit élaborer un plan de classement des données.
- **Trier régulièrement ses courriels électroniques** R3 **:** supprimer les pourriels et doublons, sauvegarder les messages importants.

- **Lorsqu'un agent est muté, change de service ou part à la retraite, il doit rendre les documents sur lesquels il travaille, plus largement toutes les données de la collectivité qui sont en sa possession** R4 **:** l'agent n'est pas propriétaire des documents qu'il produit ou reçoit dans le cadre de ses fonctions.

En règle générale, la gestion des documents numériques est similaire à celle des documents papiers : traitement au fil de l'eau, mise en place de plans de classement, éliminations selon les dispositions législatives en vigueur. **Un pré-archivage numérique peut favoriser le succès d'un projet d'archivage électronique définitif** R5. Les collectivités peuvent s'appuyer sur les 5 fiches pratiques[58] crées par les archivistes départementaux de la région Centre-Val-de-Loire, qui aideront à aiguiller les administrations souhaitant mener à bien des opérations de pré-archivage numérique.

Les archives publiques (papier ou électroniques), au sens de l'article L. 211-4 du Code du patrimoine, ainsi que les biens classés comme archives historiques en application du livre II, sont des **trésors nationaux**, et cela quelle que soit leur date et leur lieu de conservation. Sauf les exceptions prévues dans l'article L111-7 du code du Patrimoine, les trésors nationaux ne peuvent pas sortir du territoire national, cela impacte le recours à l'externalisation des archives électronique. Toutefois, le cadre juridique du tiers-archivage est en cours d'évolution. En effet, incompatible en droit avec les règlements européens relatifs à la protection générale des données et à la libre circulation des données, l'obligation de localisation des archives courantes et intermédiaires sur le territoire national doit disparaitre à partir de 2021.

Le cadre juridique actuel permet aux collectivités, sous certaines conditions et en fonction de leur statut (Régions, communes, EPCI, EPL, etc.), d'externaliser (de confier à un tiers-archiveur) ou de mutualiser leurs archives électroniques. Voici donc quelques solutions de base d'archivage électronique possibles pour une collectivité[59] :

- Mettre en œuvre un **système d'archivage électronique (SAE)** associant des outils et des procédures pour la bonne gestion des archives courantes, intermédiaires et/ou définitives.
- Déposer, par convention, les archives auprès des structures tierces. Par exemple, les communes, les EPCI, les Régions et EPL peuvent déposer leurs archives auprès du **service d'archives départemental** compétent.
- Mutualiser, par convention, la gestion des archives avec un ou plusieurs autres services publics d'archives (loi LCAP de 2016). Cette solution n'est possible que pour les collectivités dotées d'un **service public d'archives** (SPA).
- Externaliser la conservation de ses archives électroniques courantes et intermédiaires à l'aide d'un **tiers-archiveur agréé**[60]. Dans ce cas, la collectivité doit retenir une autre solution pour la conservation de ses archives électroniques définitives.

Quelle que soit la solution retenue par la collectivité, un Contrôle Scientifique et Technique (CST) sur ses archives publiques sera assuré par un représentant de l'État, qui validera ou invalidera alors la solution choisie.

58 https://www.archives-loiret.fr/que-faire-de-vos-archives/administration-officier-public/comment-gerer-des-documents-electroniques-
59 https://www.modernisation.gouv.fr/sites/default/files/dcant_rapport_detude_archivage_electronique__0.pdf
60 Prestataires agréés pour la conservation d'archives publiques courantes et intermédiaires sur support numérique : https://certificats-attestations.afnor.org/referentiel/NF461

En complément, les collectivités peuvent s'appuyer sur le programme Vitam qui est une solution logicielle libre d'archivage électronique porté par les ministères de la Culture, des Armées et de l'Europe et des Affaires Étrangères. La phase projet s'est achevé à la fin de l'année 2019, un suivi du logiciel et un accompagnement de ses utilisateurs sont assurés depuis le début d'année 2020 au moyen d'un dispositif de maintenance et d'amélioration continue (MAC Vitam) et d'un Club utilisateurs.

Réglementation, normalisation et certification

Le choix de la solution d'archivage électronique doit prendre en compte les réglementations (RGPD, eiDas, etc.), les normes et les certifications en vigueur RG :

- La **norme** française **NF Z 42-013** et son équivalent international **ISO 14641** sur le **système d'archivage électronique (SAE)** fixent le cadre à mettre en œuvre pour l'enregistrement, l'archivage et la communication de documents numériques afin d'assurer la lisibilité, l'intégrité et la traçabilité de ces documents pendant la durée de leur conservation et de leur utilisation.
- La **norme NF Z 42-020** défini les fonctions minimales que doit posséder un **composant coffre-fort numérique (CCFN)** piloté par un système d'archivage électronique et destiné à la conservation d'objets numériques dans des conditions de nature à en garantir leur intégrité dans le temps. En effet, un SAE peut intégrer nativement les fonctions de préservation de l'intégrité ou s'appuyer sur un CCFN conforme à cette norme.
- La **certification NF 461** permet de garantir que les organismes respectent les normes **NF Z42-013** et **ISO 14641** concernant le fonctionnement d'un système d'archivage électronique. La certification est délivrée par **AFNOR Certification**, l'association française de la normalisation.

Que ces archives soient internalisées ou externalisées, le recours à ces normes et certifications facilite les tâches associées au **Contrôle Scientifique et Technique de l'État** sur les archives publiques.

Cette fiche contient 6 recommandations.

Références :
https://francearchives.fr/file/f3e02b58b9f9ef87725ecf422da10422270852e0/static_7429.pdf
https://www.cdg84.fr/wp-content/uploads/2018/07/2018_Guide_archives_web.pdf
http://www.archives28.fr/_depot_image_ad28/_depot_arko/articles/1422/guide-d-archivage-pour-les-communes-et-les-groupements-de-collectivites-_doc.pdf
https://references.modernisation.gouv.fr/sites/default/files/Referentiel%20General%20de%20Gestion%20des%20Archives%20R2GA%20-%20octobre%202013.pdf
https://francearchives.fr/fr/file/8229105e7fca3fec9580af165e8de5468076601d/DPACI_RES_2009_018_maj_20170822.pdf
https://francearchives.fr/fr/file/03da67e398796d6e2d49035f014e98e995e9e00e/DGP_SIAF_2018001_mutualisation_archivage_electronique.pdf

Fiche n°11

Serveurs et locaux

La fonctionnalité principale des serveurs est de permettre aux agents et aux usagers d'avoir constamment accès aux services de l'organisation (Web, messagerie, stockage, etc.). Les serveurs sont une cible particulièrement prometteuse pour les pirates informatiques, car ils sont à la base de toutes les activités et centralisent un grand nombre de données. Les risques physiques, liés aux évènements imprévisibles comme les pannes, les accidents ou les atteintes intentionnelles aux matériels, doivent également être pris en compte lors de l'installation de serveurs[61]. Si le bon fonctionnement des serveurs est affecté, l'organisation entière peut se retrouver paralysée (interruption des processus métier, perte de données, blocage des accès aux services, etc.).

Les bonnes pratiques suivantes vous permettront de renforcer la sécurité de vos installations. La gestion de certains serveurs nécessite des compétences poussées en informatique (gestion en ligne de commandes), d'autres possèdent une interface d'administration graphique plus ou moins intuitive (serveur NAS, etc.). Ces recommandations sont générales et peuvent être appliquées aux différents types de serveurs hébergés et gérés en interne par l'organisation.

- **Sécurisez vos locaux** R1 **:**
  - Point essentiel, l'accès aux locaux doit être contrôlé, cela pour éviter ou ralentir un accès non autorisé aux serveurs, mais aussi aux divers matériels informatiques et aux fichiers papiers ;
  - Conservez une trace des accès aux salles ou aux bureaux susceptibles d'héberger du matériel contenant des données personnelles ;
  - Choisissez une pièce fermée à clé, qui comporte très peu d'ouvertures (risque d'intrusion physique) et éloignée des lieux de passage ;
  - Évitez d'installer les serveurs dans des sous-sols ou au dernier étage d'un immeuble (risques d'infiltration d'eau) ;
  - La température et l'hygrométrie des locaux où sont installés les serveurs doivent être contrôlées et stables, car un environnement trop chaud ou trop humide pourrait causer des dommages irréversibles aux composants internes des serveurs ;
  - Mettez en place des alarmes anti-intrusion, des détecteurs de fumée et des moyens de lutte contre les incendies. N'oubliez pas de les inspecter régulièrement, et au moins une fois par an ;
  - Mettez en place un onduleur afin de protéger vos serveurs d'une panne de courant ou de surtensions ;
  - Entretenez vos installations, car les risques peuvent provenir de pannes ou de dysfonctionnements liés à leur vétusté (climatisation, tableau électrique, etc.) ;

61 http://www.digne.cci.fr/IMG/pdf/Fiche_27_-_Securite-Mettre_son_serveur_en_securite.pdf

- **Activez le pare-feu et installez un logiciel anti-virus sur les serveurs** R2 **:** par défaut, le pare-feu présent sur un serveur ne possède aucune règle active. Créez et ajustez des règles de pare-feu en fonction du service et de l'utilisation du serveur. Pensez à installer sur vos serveurs une solution anti-virus différente de celle installée sur les postes clients. Utilisez des logiciels scanner et des outils de détection des vulnérabilités.

- **Interdisez ou sécurisez les connexions distantes aux serveurs** R3 **:** certains services ne doivent jamais être accessibles directement de l'extérieur (serveur de sauvegarde, bases de données, etc.). A l'inverse, quand le but même du service est d'assurer les connexions ou requêtes distantes (serveur VPN, serveur Web, etc.), vous devez limiter et sécuriser ces accès :
  - Mettez en œuvre les moyens de connexion et les protocoles sécurisés (VPN, SSH, TLS[62], https, etc.).
  - Lorsque cela est possible, n'accordez les accès distants qu'aux comptes et aux adresses IP spécifiques.
  - Bloquez les accès distants aux comptes administrateurs ou à ceux ayant des privilèges élevés.
  - Activez la double authentification si la technologie que vous utilisez vous le permet.

- **Désactivez les comptes existants par défaut et évitez les noms d'utilisateur trop communs** R4 **:** une partie des tentatives d'intrusion aux serveurs se fait avec un nom d'utilisateur connu ou crée par défaut. Désactivez les comptes par défaut, comme « admin » et « user ». Pour administrer votre serveur, créez un nouveau compte avec les privilèges adéquats nécessaires, en évitant les noms tels que « admin », « administrateur » ou « root ».

- **Mettez en place une politique de gestion des droits d'accès aux ressources** R5 **:** attribuez le minimum de privilèges nécessaires au bon fonctionnement d'un service sur un serveur spécifique. Il est également important d'appliquer le principe du moindre privilège aux utilisateurs. Seuls les agents ayant un besoin légitime en lien avec leur mission doivent pouvoir accéder aux serveurs.

- **Créez un compte par utilisateur** R6 **:** chaque agent doit disposer d'un identifiant propre et nominatif et d'un mot de passe personnel qu'il doit protéger (voir la fiche 3 « Mots de passe »). Deux (ou plusieurs) personnes ne doivent jamais utiliser/partager le même compte.

- **Effectuez les mises à jour de manière régulière** R7 **:** mettez à jour le système d'exploitation de chaque serveur, ainsi que tous les logiciels qui y sont installés, appliquez les derniers correctifs de sécurité. N'installez jamais les versions « beta » des mises à jour. Ces versions ne sont pas stables et peuvent comporter des bogues.

- **Supprimez ou désactivez les modules et paquets inutiles** R8 **:** tout comme sur votre poste de travail, de nombreux logiciels sont installés par défaut sur

62 https://www.ssi.gouv.fr/uploads/2017/07/anssi-guide-recommandations_de_securite_relatives_a_tls-v1.2.pdf

un serveur. Gardez à l'esprit que plus le nombre de services fonctionnant sur un système d'exploitation est grand, et plus il y a de possibilités pour l'attaquant de profiter d'une vulnérabilité de votre système. Seuls les logiciels, services ou modules strictement nécessaires au bon fonctionnement du serveur doivent y être installés.

- **Séparez les services et les environnements** R9**,** en particulier :
  - Les serveurs hébergeant les bases de données ou traitant des données sensibles ne doivent jamais être utilisés pour d'autres fonctions (serveur Web, messagerie, etc.).
  - Sur un serveur Web, les fichiers de site Web et les scripts doivent toujours être séparés du système d'exploitation, être sur une autre partition.
  - Les applications Web en cours de développement ne doivent jamais utiliser ou se connecter à des bases de données en production.

- **Activez les notifications et surveillez les journaux** R10 **:** activez les messages d'alertes et inspectez les journaux (logs), ils permettent de retracer l'activité des utilisateurs et des serveurs ; cela fait partie des règles de base de la sécurité.

- **Définissez le plan et la stratégie de sauvegarde** R11 **:** automatique ou manuelle, sur quel support et à quelle fréquence (voir la fiche « Plan et stratégies de sauvegarde »). Pensez également à sauvegarder les configurations des serveurs.

Afin de comprendre, configurer et sécuriser les services les plus visés, mais aussi pour aller plus loin, vous pouvez vous appuyer sur les documentations et les notes techniques suivantes :

CNIL : « Sécurité des sites web : les 5 problèmes les plus souvent constatés »[63],

ANSSI : « Recommandations pour la sécurisation des sites web »[64], « Recommandations pour un usage sécurisé d'(Open)SSH »[65],

« Comprendre et anticiper les attaques DDoS »[66],

« Recommandations de configuration d'un système GNU/Linux »[67], « Recommandations relatives à l'administration sécurisée des systèmes d'information »[68].

Cette fiche contient 11 recommandations.

Références :

http://www.wikayanet.dz/images/Guides/guide12-2.pdf
https://www.cnil.fr/fr/securite-securiser-les-serveurs
https://www.cnil.fr/fr/securite-proteger-les-locaux
http://www.digne.cci.fr/IMG/pdf/Fiche_27_-_Securite-Mettre_son_serveur_en_securite.pdf

63 https://www.cnil.fr/fr/securite-des-sites-web-les-5-problemes-les-plus-souvent-constates
64 https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Securite_Web_NoteTech.pdf
65 https://www.ssi.gouv.fr/uploads/2014/01/NT_OpenSSH.pdf
66 https://www.ssi.gouv.fr/uploads/2015/03/NP_Guide_DDoS.pdf
67 https://www.ssi.gouv.fr/uploads/2016/01/linux_configuration-fr-v1.2.pdf
68 https://www.ssi.gouv.fr/uploads/2015/02/guide_admin_securisee_si_anssi_pa_022_v2.pdf

N°12

Fiche n°12

Externalisation

Diverses raisons peuvent motiver une organisation à externaliser (confier) la gestion de tout ou partie de son système d'information à des organismes sous-traitants, par exemple, l'absence des compétences nécessaires en informatique en interne ou pour des raisons budgétaires. Toutefois, le recours à la sous-traitance n'est pas une option sans risque, notamment en ce qui concerne la gestion des données à caractère personnel. En effet, l'organisation est responsable des données qu'elle détient et cela même si elle a un recours à un sous-traitant. Elle est donc dans l'obligation de s'assurer du bon traitement de ces données par ses sous-traitants, aussi dans le strict cadre du règlement RGPD.

Les recommandations suivantes permettront aux organisations de bien démarrer leur processus d'externalisation :

- **Réaliser une analyse de risques** R1 **:** vous pourrez ainsi exiger du prestataire qu'il applique les mesures de sécurité appropriées, à mettre en œuvre au sein de l'organisation, qui découlent de cette analyse (voir le chapitre final « Mener une analyse de risques »).

- **Définir clairement les ressources à externaliser** R2 **:** identifier les équipements, les outils logiciels et les données qui sont concernés par la sous-traitance, définir les différents niveaux de services attendus, dans le but de convenir d'un budget de référence.

- **Demander explicitement aux prestataires répondant à l'appel d'offres un plan d'assurance sécurité (PAS)** R3 **:** ce document, à la fois juridique et technique, décrit l'ensemble des dispositions spécifiques que la société sous-traitante s'engage à mettre en œuvre pour garantir le respect des règles de sécurité informatique imposées par le client. Il facilite également la comparaison des offres. Une fois le prestataire retenu, le PAS doit être annexé au contrat et peut alors remplacer les clauses génériques de sécurité de ce dernier.

- **Choisir un prestataire** R4 **:** faites appel uniquement à des sous-traitants qui sont soumis à la règlementation de l'Union européenne et au respect des principes européens en matière de protection des données personnelles, et de la loi Informatique et Libertés. **Privilégiez les prestataires qualifiés par l'ANSSI** pour chaque typologie de besoins, par exemple SecNumCloud pour le stockage des données en externe. Les collectivités peuvent aussi s'appuyer sur les structures d'achats publics groupés, telle l'UGAP.

Lorsqu'il s'agit d'externaliser le traitement des données de santé[69], le sous-traitant doit être titulaire d'un certificat de conformité délivré par des organismes de certification accrédités par l'instance française d'accréditation : la certification Hébergement des Données de Santé (HDS).

- **Établir un contrat clair et précis** R5 **:** on désigne un contrat de sous-traitance informatique par le terme d'infogérance. Comme dans tout contrat qui se forme entre deux parties, le contrat d'infogérance doit définir :
  - L'identification du prestataire et du client ;
  - La date de formation, la durée initiale, le renouvellement et les modalités de résiliation ;
  - La facturation, les modalités de règlement et l'évolution tarifaire ;
  - Les responsabilités des deux parties ainsi que des clauses particulières.

Certains contrats de prestataires n'offrent pas les garanties nécessaires, d'autres refusent toute négociation quant aux clauses du contrat : pour rester en conformité avec la législation en vigueur il ne faudra en aucun cas sélectionner de tels prestataires ! En amont de la signature, les organisations peuvent faire analyser le contrat par des spécialistes techniques et juridiques. Rappelez-vous qu'il s'agit d'un contrat par lequel vous autorisez une société tierce à entrer dans votre système informatique et à manipuler vos données et celles de vos administrés.

- **Inclure des clauses de sécurité dans le contrat** R6 **:**
  - Les clauses liées aux contraintes légales : la localisation des données, la garantie de sécurité et de confidentialité, les réglementations spécifiques à certains types de données, notamment dans le cadre de traitement par un sous-traitant des données à caractère personnel les mentions particulières obligatoires[70] doivent être incluses dans le contrat ;
  - Les clauses liées aux contraintes pratiques : les délais de prise en compte des incidents, les moyens d'intervention, d'assistance (hotline, téléphonique, présentiel), les horaires et les jours d'intervention, les tarifications supplémentaires ;
  - La clause de transparence : si le prestataire fait appel lui-même à un sous-traitant, une autorisation explicite doit être demandée à l'organisation ;
  - La clause de réversibilité et de résiliation du contrat : permet de changer de prestataire plus simplement.

Ces clauses sont générales et ne sont pas exhaustives. L'organisation doit inclure dans le contrat les clauses appropriées à la typologie de sous-traitance dont elle a besoin.

69 Le traitement des données de santé est encadré par l'article L 1111-8 du Code de la santé publique et par le RGPD.
70 https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article28

N°12

Les contrats d'hébergement souscrits par des entités publiques bénéficient d'un droit de rupture anticipée[71], tel que prévu par le Cahier des clauses administratives générales (CCAG) relatif aux Techniques de l'Information et de la Communication (TIC). Il ne faut pas hésiter à changer de prestataire si celui-ci ne correspond pas aux exigences de la collectivité.

N'oubliez pas de changer les mots de passe des services auxquels les anciens fournisseurs avaient accès, changer de fournisseur c'est aussi changer les mots de passe des différents services que le prestataire opérait, tout comme vous le faites après le départ d'un agent ou d'un stagiaire.

Pour aller plus loin, les collectivités peuvent s'appuyer sur le guide « Maitriser les risques de l'infogérance »[72] rédigé par l'ANSSI.

Cette fiche contient 6 recommandations.

Références :

https://www.ssi.gouv.fr/uploads/2020/01/anssi-guide-securite_numerique_collectivites_territoriales-reglementation.pdf
https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf
https://www.decision-achats.fr/Thematique/achats-publics-1230/Breves/Tribune-Quelle-strategie-Cloud-secteur-public-333910.htm

71 https://www.decision-achats.fr/Thematique/achats-publics-1230/Breves/Tribune-Quelle-strategie-Cloud-secteur-public-333910.htm
72 https://www.ssi.gouv.fr/uploads/IMG/pdf/2010-12-03_Guide_externalisation.pdf

MENER UNE ANALYSE DE RISQUES _

MENER UNE ANALYSE DE RISQUES

En matière de sécurité, l'union fait bien la force. Chaque agent qui applique les bonnes pratiques données dans ce guide et qui reste en éveil sur celles de ses collègues, participe au quotidien à la sécurité globale de son service. Au-delà des matériels et logiciels utilisés, au-delà des routines quotidiennes, ce guide est l'étape liminaire qui permettra à tout administrateur de mieux évaluer quelles sont les vulnérabilités de son système d'information (SI) au regard des inconvénients ou dangers plus ou moins probables auxquels il peut être exposé, afin qu'il prenne les meilleures mesures pour le protéger. L'analyse de risques est un outil structurant qui permettra à l'organisation de gérer au mieux les risques pour réduire au maximum son exposition aux menaces.

Qu'est-ce que le risque ?

En informatique, le risque est la possibilité de survenue d'un événement indésirable qui génère un préjudice portant atteinte à l'un des composants du système d'information ou de son environnement, par exemple la perte ou le vol de données, la dégradation d'un service ou un sabotage pouvant aller jusqu'à l'arrêt du système ou des applications, les conséquences en terme d'image ou juridiques.

Quatres facteurs entrent en jeu dans l'**évaluation du risque** :

- **La vulnérabilité :** c'est une faiblesse ou une faille au regard de la sécurité du système d'information (SI composé de deux sous-systèmes, l'un **social**, composé de la structure organisationnelle et des personnes liées au SI, et l'autre **technique**, composé des technologies et des processus d'affaires concernés par le SI) ;

- **La menace :** elle exploite une vulnérabilité du SI, selon un scénario de menace précis, son action amène une dégradation ou la destruction du SI, des services qu'il rend et des données qu'il contient, elle peut être d'origine humaine, volontaire ou involontaire, ou résulter de phénomènes non humains (animal, végétal, climatique, physique) ;

- **La probabilité** qu'une vulnérabilité soit exploitée par une menace ;

- **L'impact :** évalue les conséquences physiques, financières (dommage corporel et/ou matériel), juridiques, ou concernant la réputation (dommage moral), aussi vis-à-vis des usagers (indisponibilité d'un service, défiguration du site Web, vol, revente, exposition de données à caractère personnel), etc.

Qu'est-ce qu'une analyse de risques ?

Dans le domaine de la sécurité informatique, une analyse de risques est un processus d'identification (composants du SI et schéma des flux), d'évaluation et d'estimation de chaque composante du risque (vulnérabilité/scénarii de menace/probabilité/impact) liée au SI. Cette analyse permettra à l'organisation de déterminer quel niveau de risque est acceptable pour elle au regard du budget qui est dédié à sa sécurité, elle pourra alors prendre les mesures adéquates pour couvrir les risques jugés inacceptables et protéger ainsi les biens et services essentiels de l'organisation, à commencer par les données.

Quand faut-il mener une analyse de risques ?

De nombreux facteurs peuvent motiver la réalisation d'une telle analyse. Par exemple, chaque fois que des changements importants interviennent dans l'environnement informatique, comme l'ajout ou la suppression de matériel et/ou de logiciels, avant l'ouverture d'un téléservice, avant d'externaliser tout ou une partie de la gestion du système d'information, en complément d'un audit de sécurité[73]. Une analyse de risques devient indispensable lorsque le système est critique pour la productivité et/ou traite, stocke ou transmet des données sensibles.

Comment mener une analyse de risques ?

L'évaluation des risques peut se limiter à une analyse d'écart par rapport à la réglementation applicable (RGS, RGPD, etc.) et aux guides de sécurité informatique existants (ce guide, « Guide d'hygiène informatique »[74] de l'ANSSI, etc.). Il existe toutefois différentes méthodes qui permettent de réaliser une analyse de risques (EBIOS, MEHARI, OCTAVE, etc.), et votre choix sera fonction de la criticité du système à analyser. Les grandes administrations doivent utiliser la méthode Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS).

L'Agence nationale de la sécurité des systèmes d'information élabore et tient à jour un important référentiel méthodologique « La méthode EBIOS Risk Manager » destiné à aider les organismes du secteur public et du secteur privé à gérer la sécurité de leurs systèmes d'informations. Ce référentiel est composé de méthodes, des meilleures pratiques et de logiciels, il est diffusé gratuitement sur le Internet de l'ANSSI[75] et nous le recommandons.

La CNIL a élaboré trois guides[76] autour de l' « Analyse d'impact relative à la protection des données », qui portent respectivement sur la méthode, les modèles et les bases de connaissances, et qui décrivent la manière d'employer la méthode EBIOS dans le contexte spécifique de la Loi « Informatique et libertés ».

73 Réalisé par un organisme extérieur et certifié, un audit de sécurité permet d'obtenir une vision du système d'information à un moment précis, et d'en comparer l'état au regard d'un référentiel (RGS, RGPD, règles et textes de loi), afin d'aider l'organisation à prendre les bonnes décisions.

74 https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

75 https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/

76 https://www.cnil.fr/fr/gerer-les-risques

En interne, un groupe de travail qui ne serait pas dédié à la technique et qui impliquerait tous les acteurs du système d'information pourrait réaliser les étapes essentielles d'une analyse de risques. Cela permettrait à l'organisation de mieux appréhender les enjeux de sécurité de son SI tout en réalisant des économies. Après avoir produit une première analyse, l'organisation pourra faire appel à une société extérieure chargée d'approfondir chaque point soulevé par le travail fait en interne.

Les étapes suivantes, accompagnées d'un exemple fil rouge simple, permettront d'évaluer et de gérer les risques :

Cartographier le système d'information et identifier les exigences en matière de sécurité :

Il est impossible de prendre des décisions stratégiques pour la sécurité du système d'information si les ressources informatiques et les données à protéger ne sont pas identifiées. La cartographie du système d'information permet d'obtenir une vision globale de son patrimoine informatique, matériel et immatériel. Pour cartographier votre système, vous pouvez vous appuyer sur des outils et documentations existants, par exemple, le guide « Cartographie du système d'information »[77] proposé par l'ANSSI.

Après avoir identifié les ressources à protéger, il faut déterminer les exigences de sécurité qui leurs sont associées, dont les plus essentielles sont :

- **La disponibilité :** les ressources doivent être accessibles et utilisables par les personnes autorisées aux moments voulus ;
- **La confidentialité :** les ressources ne sont accessibles qu'aux personnes autorisées ;
- **L'intégrité :** les ressources ne sont modifiées ou supprimées que par des personnes autorisées à le faire et selon une procédure bien définie ;
- **La traçabilité :** la garantie que les accès et tentatives d'accès aux ressources sont bien tracés et que ces traces sont conservées et exploitables.

Un serveur Web hébergé en interne de l'organisation aura un besoin d'être disponible, alors que les données contenues dans une base de données exigera avant tout confidentialité et intégrité.

77 https://www.ssi.gouv.fr/uploads/2018/11/guide-cartographie-systeme-information-anssi-pa-046.pdf

Identifier quelles sont les vulnérabilités et les contre-mesures associées :

Une vulnérabilité est une faiblesse d'un composant du SI qui le rend sensible à une menace. Pensez d'abord aux vulnérabilités physiques : tels des locaux mal sécurisés, la vétusté du système électrique, etc. Puis aux mauvaises configurations logicielles, aux accès trop permissifs, aux mots de passe trop faibles, aux logiciels non mis à jour, etc.

Une contre-mesure permet quant à elle de minimiser ou de supprimer la possibilité d'exploiter une vulnérabilité du système, par exemple, la bonne configuration d'un pare-feu, des sauvegardes régulières, un contrôle des accès, un changement régulier des mots de passe, etc.

Il existe de nombreuses pratiques pour détecter les vulnérabilités des systèmes d'information, par exemple, les analyses anti-virus, les logiciels scanneurs de vulnérabilités (tels que Nmap, Nessus, Nikto, etc.), la veille technologique auprès de sources d'informations fiables (éditeurs, sites spécialisés, CERT-FR[78]), les alertes et suggestions remontées par les agents ou les administrés, les audits de sécurité.

Un serveur Web hébergé en interne peut être vulnérable, à cause de la vétusté du système de climatisation, du fait que la salle des serveurs est en sous-sol, etc. A l'inverse des contre-mesures peuvent venir contrer certaines menaces, tel un pare-feu installé et configuré.

Identifier les menaces :

Les menaces sont la somme tout ce qui pourrait potentiellement exploiter les vulnérabilités du SI, porter atteinte à la sécurité de l'organisation et lui causer grand tort. Les menaces sont de différents types, elles sont énumérées dans le tableau ci-dessous.

SOURCE : interne/externe	**GRAND TYPE DE MENACE**
HUMAINE	**Malveillance :** espionnage, sabotage, déstabilisation, cybercriminalité
	Erreur accidentelle : perte/suppression des données, virus non ciblé,...
NON HUMAINE	**Phénomène électrique :** panne, incendie, explosion,...
	Phénomène environnemental : inondation, tempête, rongeurs,...

Gardez à l'esprit que les catastrophes naturelles, les pannes ou les erreurs humaines non intentionnelles peuvent impacter aussi fortement le SI (parfois plus) que la malveillance des pirates et les virus, ces derniers étant certes plus médiatiques.

78 https://www.cert.ssi.gouv.fr/

Et s'il s'agit d'une malveillance, il ne faut pas confondre :

- **La cible d'une attaque :** un élu, un employé qui a accès à de nombreuses informations, par exemple ;

- **Le moyen d'en connaître :** des recherches effectuées en amont par l'attaquant sur des sources ouvertes, sur les réseaux sociaux, dans des articles de journaux, des vidéos, qui concernent une personne publique, son image, ses fréquentations, ses déplacements, ses centres d'intérêts et opinions, son entreprise, ses voyages, etc.

- **Le moyen de mener l'attaque :** par un message électronique, une pièce jointe, en infectant un logiciel, avec une clé USB, etc.

- **La charge active :** virus, ver, cheval de Troie, etc.

Notre serveur Web interne peut subir une attaque DDoS qui va le rendre indisponible quelques heures, une injection SQL qui va permettre au pirate d'en prendre le contrôle, etc.

Évaluer la probabilité d'un incident et la gravité de son impact :

À chaque menace identifiée correspondent deux indicateurs, la probabilité qu'une vulnérabilité soit effectivement exploitée et la gravité de l'impact de l'action de cette menace pour l'organisation. Afin d'évaluer ces deux indicateurs, vous pouvez utiliser une échelle de valeurs relatives (1, 2, 3) ou des catégories (faible, moyen, élevé). Il semble impossible, voire dangereux, d'affirmer avec certitude qu'un de ces indicateurs soit égal à 0 (ou absent) : la valeur 0 ne doit pas être utilisé.

La probabilité et l'impact sont évalués en tenant compte de tous les facteurs identifiés durant les étapes précédentes, tel le type de la vulnérabilité (matérielle, logicielle, physique, humaine), l'existence (ou non) de contre-mesures, les capacités et la motivation d'un l'individu, la base de connaissance des incidents précédents. Chacun de ces éléments peut être la source de nombreux risques, qui peuvent aussi s'enchaîner et se combiner en des scénarii complexes mais réalistes.

La salle qui héberge le serveur Web interne de l'organisation peut être en sous-sol et de fortes pluies sont prévues. L'impact d'une potentielle inondation du sous-sol serait d'ordre financier (rachat d'un nouveau matériel) ou juridique (responsabilité si perte de données). Toutefois, si le bâtiment est construit en zone non inondable, la probabilité d'un tel incident est alors réduite au minimum.

Évaluer et classer les risques :

Croiser ces deux indicateurs, la probabilité et l'impact, permet d'ordonner les risques ; par exemple, un risque sera considéré comme élevé si la somme des valeurs de la probabilité et de l'impact est comprise entre 5 ou 6 ; le risque sera dit moyen si cette somme est comprise entre 3 et 4, faible ou pouvant être toléré si la somme est comprise entre 2 et 3.

En combinant les scénarios de menaces et les événements redoutés, nous pouvons dresser le tableau non-exhaustif ci-dessous qui permet d'identifier et de classer une partie des risques qui pèsent sur notre serveur Web interne.

MENACE	VULNÉRABILITÉ/ CONTRE-MESURES	PROBA-BILITÉ	IMPACT	RISQUE
SURCHAUFFE	Le système de climatisation est vétuste	**3**	Financier : **3**	**Élevé :** rachat du matériel
INONDATION	Serveur installé au sous-sol / Zone non inondable	**1**	Financier, juridique : **2/3**	**Moyen :** peu probable
ATTAQUE DDoS	Pare-feu installé et configuré	**1**	Indisponibilité temporaire du service : **1**	**Faible**

Gérer les risques :

Après avoir évalué et classé les risques qui ont été identifiés, plusieurs démarches ou mécanismes sont possibles pour les gérer :

- **Traiter :** mettre en place des moyens techniques (chiffrement, mécanismes de détection d'intrusion, etc.) ou non techniques (telles qu'une politique de sécurité, des mesures administratives, etc.) ;
- **Éviter :** traiter les risques en amont ;
- **Limiter les impacts :** mettre en place un Plan de Continuité d'Activité (PCA) ou un Plan de Retour à l'Activité (PRA) ;
- **Transférer :** prendre une assurance, transférer une activité à un prestataire ;
- **Accepter :** seulement lorsque les risques sont faibles et que vous jugez être en mesure d'en gérer les conséquences.

Enfin, lorsque vous examinez les mesures visant à atténuer chaque risque, de nombreux aspects doivent être pris en compte, tels par exemple la faisabilité, le coût-avantage, les réglementations ou l'impact opérationnel.

Références :

https://www.nmayer.eu/publis/NMA-JPH_MISC24.pdf
https://blog.netwrix.fr/2019/04/03/comment-realiser-une-evaluation-des-risques-informatiques/
https://www.cnil.fr/sites/default/files/typo/document/CNIL-Guide_Securite_avance_Methode.pdf
https://amsn.gouv.mc/var/amsn/storage/original/application/cefc809070faef50a7ce627a2f739808.pdf
https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf

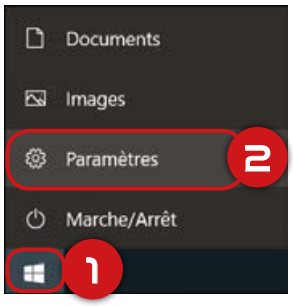
TUTORIELS _

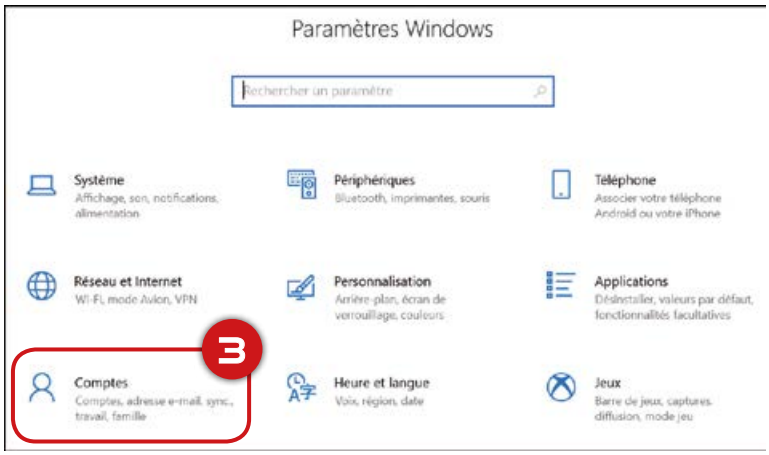
Créer un compte utilisateur standard

(+ Vidéo)

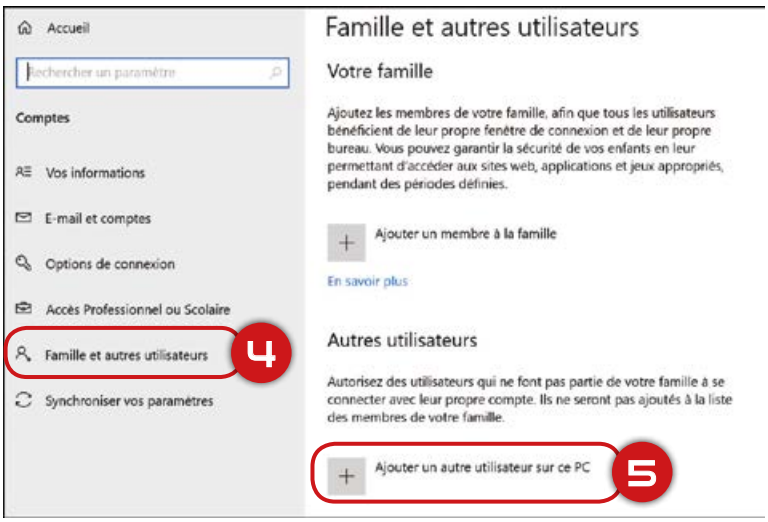
La première chose à faire pour sécuriser votre ordinateur est de créer un compte avec les droits limités. Dans Microsoft Windows cette session s'appelle utilisateur standard. Pour créer un compte d'utilisateur standard vous devez être connecté à l'aide d'un compte ayant des droits administrateur.

Cliquez sur le bouton **Démarrer** ❶, ouvrez les **Paramètres** de Windows ❷, puis choisissiez le menu **Comptes** ❸ :



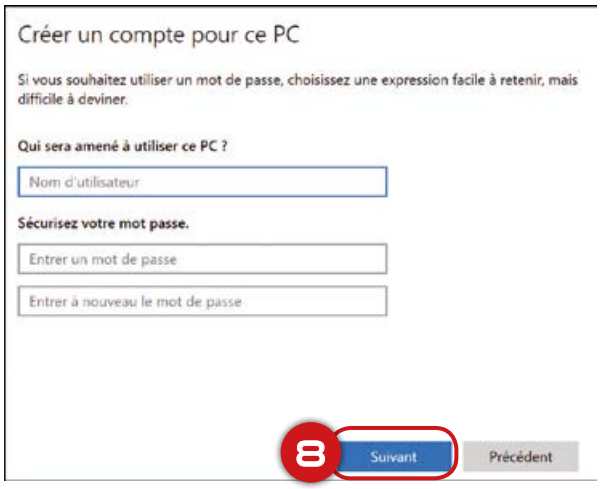


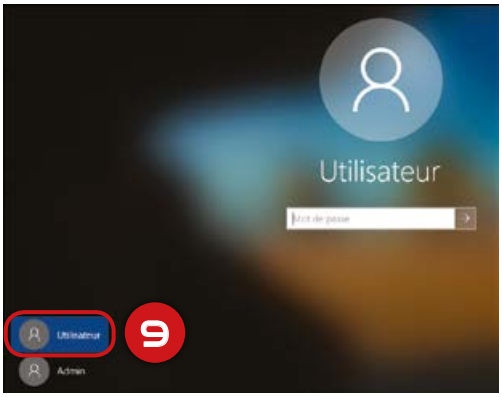
Dans la barre de menu latérale, choisissez **Famille et autres utilisateurs** ❹ (dans certaines éditions de Windows, vous verrez **Autres utilisateurs**), puis dans la zone Autres utilisateurs cliquez sur **Ajouter un autre utilisateur sur ce PC** ❺ :



Dans une nouvelle fenêtre qui s'affiche, cliquez sur **Je ne dispose pas des informations de connexion de cette personne** 6, puis sur la page suivante, choisissez **Ajouter un utilisateur sans compte Microsoft** 7 :

Entrez un nom d'utilisateur et un mot de passe (dans certaines éditions de Windows, vous serez également invité à choisir les questions de sécurité), puis sélectionnez **Suivant** 8. Vous allez être déconnecté de votre session actuelle, puis le nouveau compte créé s'affichera en bas à gauche de l'écran de connexion 9. Sélectionnez le compte nécessaire et connectez-vous à l'aide de votre mot de passe :





Lors de la création de votre espace de travail, qui peut durer plusieurs minutes, vous allez être invité à paramétrer certaines fonctionnalités de Windows, par exemple, l'utilisation de la reconnaissance vocale et linguistique, la localisation, l'utilisation de l'identifiant de publicité unique. Nous vous recommandons de ne pas activer ces fonctionnalités. Pour les désactiver ultérieurement, reportez-vous aux tutoriels correspondants.

Attention : faire des réponses simples à des questions secrètes qui concernent votre vie privée est risqué. Nous vous conseillons donc de ne pas donner les bonnes réponses à ces questions, de ne pas se contenter d'un simple mot, idéalement de mettre ici aussi un mot de passe fort !

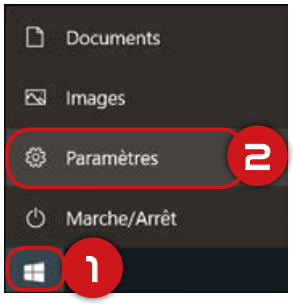
Se connecter à Windows 10 avec un compte local

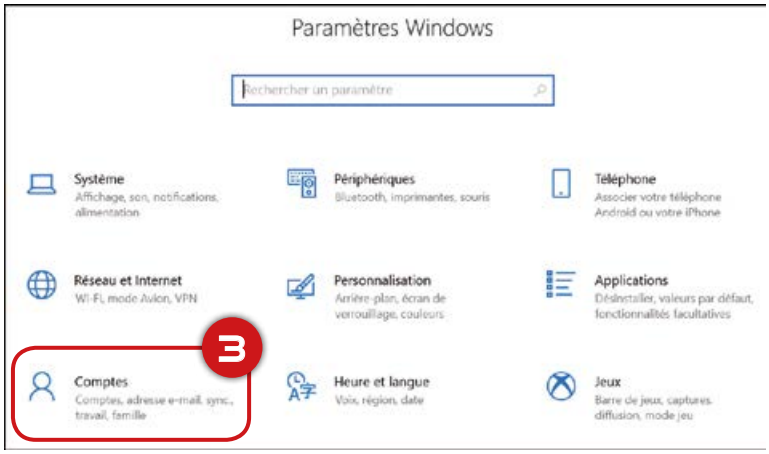
(+ Vidéo)

Nous vous recommandons de ne pas se connecter à votre système à l'aide d'un compte Microsoft. En utilisant ce service, certains paramètres de votre ordinateur (y compris les mots de passe) seront stockés sur les serveurs appartenant à Microsoft. En outre, ce type de compte est connecté aux nombreux services Microsoft qui collectent et renvoient vos données personnelles à Microsoft et ses filiales.

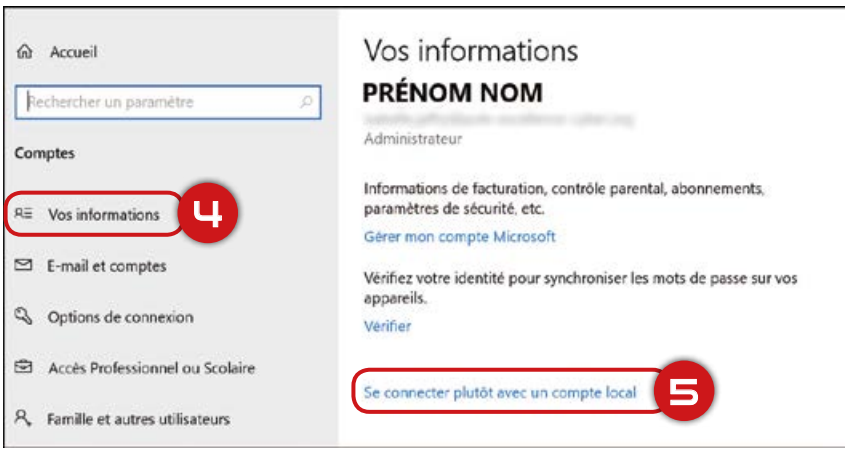
Pour basculer d'un compte Microsoft vers un compte local, tout d'abord, enregistrez votre travail (fermez vos documents), car vous allez être déconnecté de votre compte à un moment donné.

Cliquez sur le bouton **Démarrer** ❶, puis sur **Paramètres** ❷. Dans la fenêtre de **Paramètres Windows** cliquez sur **Comptes** ❸ :

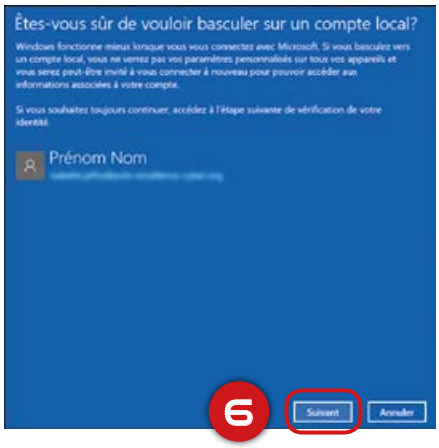


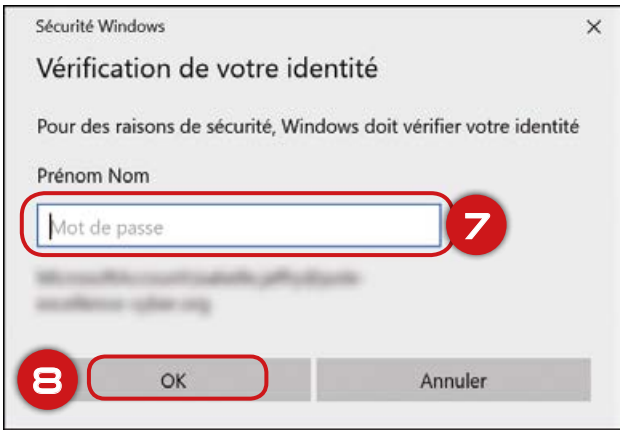


Dans la barre de menu latérale, choisissez **Vos informations** ❹, puis **Se connecter plutôt avec un compte local** ❺ :

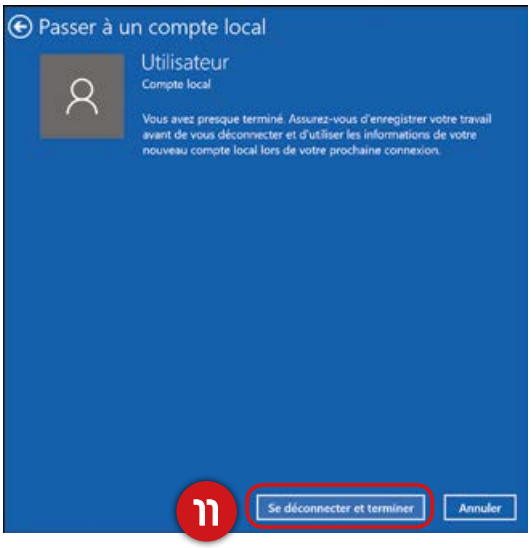


Une nouvelle fenêtre vous invite à confirmer votre choix. Cliquez sur **Suivant** 6, entrez le mot de passe associé à votre compte Microsoft 7, puis validez 8 :





Dans la nouvelle fenêtre qui s'affiche, saisissez le nom de l'utilisateur et le mot de passe pour créer un nouveau compte local 9, cliquez sur **Suivant** 10, puis sur **Se déconnecter et terminer** 11 :

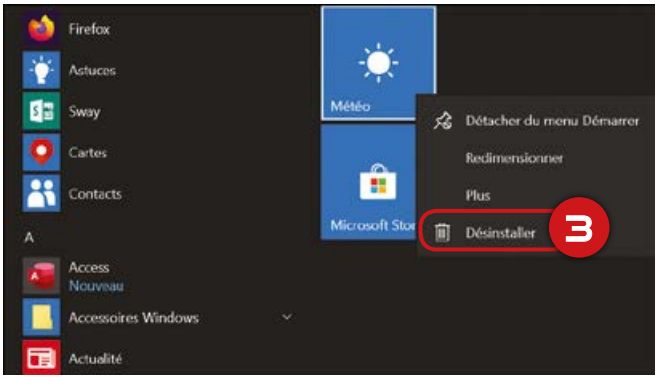


Vous allez vous déconnecter automatiquement de votre compte, puis vous pourrez vous connecter à l'aide de votre nouveau compte local dans lequel vous retrouverez toutes vos applications, vos documents et vos préférences système. Notez que ce compte possède par défaut les droits administrateurs, pensez donc à créer un compte d'utilisateur standard pour une utilisation quotidienne (vor le tutoriel « Créer un compte utilisateur standard »).

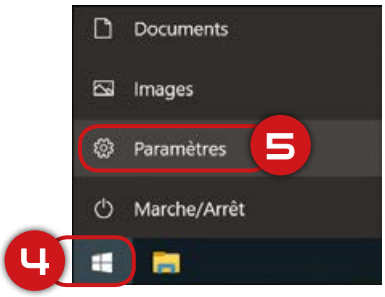
Désinstaller les applications

Par défaut, Windows 10 est fourni avec un nombre d'applications préinstallés dont certaines peuvent s'avérer inutiles. Il existe différents moyens de supprimer ces applications. La liste des applications de bureau classiques (téléchargés depuis Internet) et des applications du Microsoft Store préinstallées est accessible via le bouton **Démarrer** ❶.

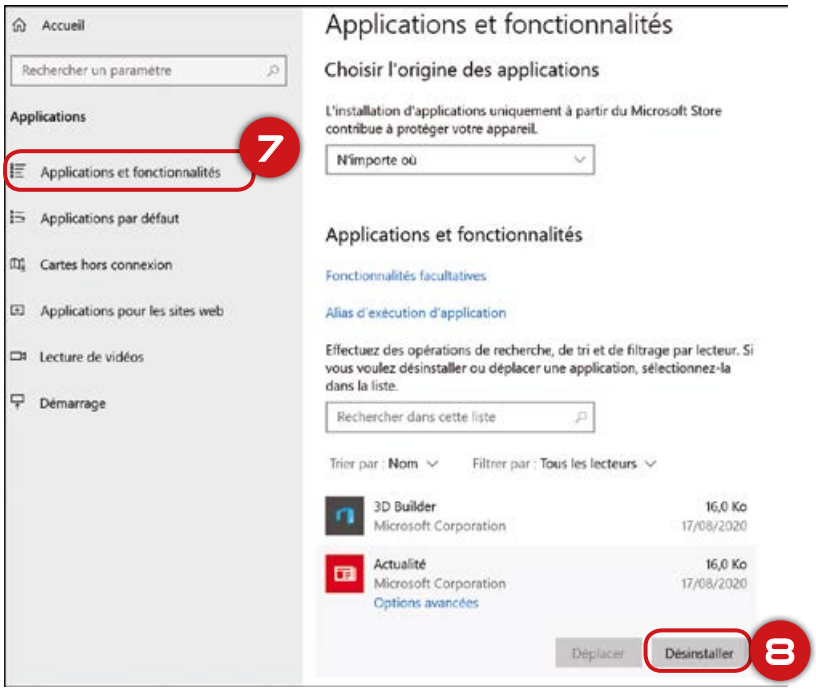
Faites un clic droit sur l'application de cette liste que vous voulez désinstaller et choisissez **Désinstaller** ❷. Certaines applications s'affichent sous forme de vignettes à droite de cette liste. Vous pouvez également les désinstaller. Pour cela, faites un clic droit sur l'application (par exemple, Météo) et choisissez **Désinstaller** ❸ :



Une autre manière d'accéder à la liste d'applications est de passer par le bouton **Démarrer** ❹, puis **Paramètres** ❺. Dans la fenêtre des paramètres Windows choisissez **Applications** ❻ :



Dans la barre de menu latérale, choisissez **Applications et fonctionnalités** 7. Cliquez sur l'application que vous voulez désinstaller, puis sur le bouton **Désinstaller** 8 :

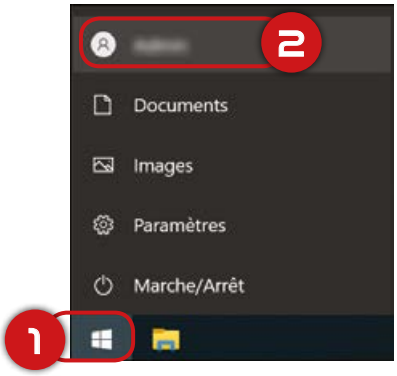


Notez que certains logiciels sont intégrés à Windows et ne peuvent pas être désinstallés. Dans ce cas, le bouton **Désinstaller** sera grisé.

Il arrive que l'application à désinstaller ne soit pas visible dans cette liste. Dans ce cas, choisissez **Programmes et fonctionnalités** 9, en fonction de la largeur de votre fenêtre, ce bouton peut se trouver tout en bas de la fenêtre courante ou sur le côté à droite. Une nouvelle fenêtre s'ouvre, il suffit de sélectionnez le programme que vous voulez désinstaller, puis de cliquer sur le bouton **Désinstaller** 10 :

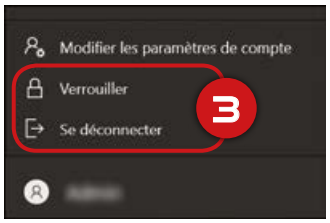
Fermer la session

Déconnectez-vous de votre session dès que vous vous éloignez de votre ordinateur. C'est un moyen facile d'empêcher une personne curieuse ou malveillante d'accéder à votre système et vos données.

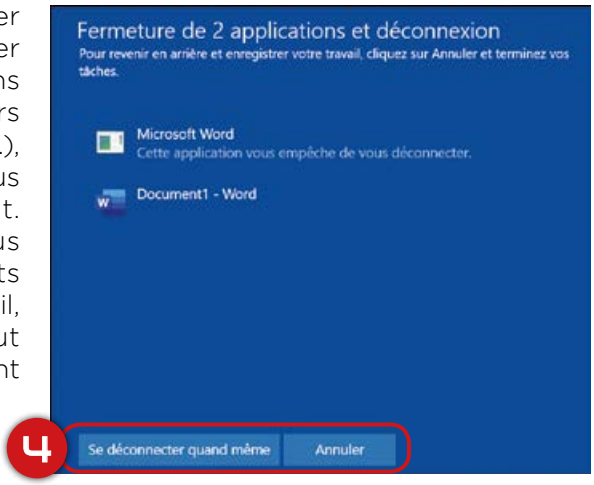


Cliquez sur **Démarrer** ❶ et choisissez votre compte utilisateur ❷ :

Vous pouvez alors vous déconnecter ou verrouiller votre session ❸ :



Si vous choisissez de vous déconnecter de votre session, le système va fermer toutes les applications ouvertes. Dans ce cas, si vous avez des tâches en cours (document Word non enregistré, etc.), le système vous en avertira et ne vous déconnectera pas automatiquement. Faites donc attention à ne pas vous précipiter. Sauvegardez vos documents avant de quitter votre poste de travail, car une personne malveillante peut accéder à votre ordinateur en annulant la fermeture de la session ❹ :

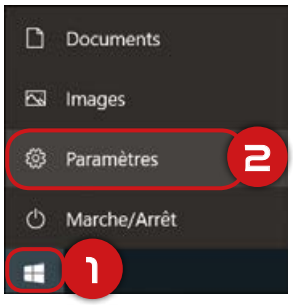


Si vous devez quitter votre poste de travail en urgence, verrouiller simplement votre session. Pour cela, il existe également un raccourci clavier : appuyez sur la touche « Windows » de votre clavier, puis, tout en maintenant enfoncée, pressez la touche « L ».

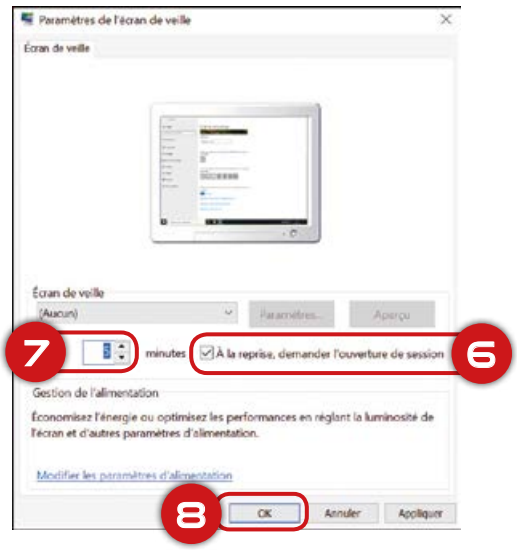
Vos applications et vos documents ouverts ne seront pas fermés par le système. Pensez tout de même à enregistrer votre travail avant de verrouiller votre session, car en votre absence, la batterie de votre ordinateur peut se décharger.

Verrouiller automatiquement la session

Vous pouvez configurer votre ordinateur pour qu'il verrouille automatiquement votre session dès que l'écran de veille s'affiche. Pour cela, cliquez sur le bouton **Démarrer** 1, puis **Paramètres** 2. Dans la fenêtre des paramètres Windows choisissez **Personnalisation** 3 :



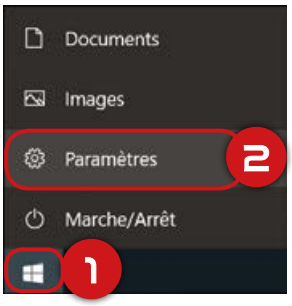
Dans la barre de menu latérale, choisissez **Ecran de verrouillage** 4. Descendez tout en bas de la fenêtre et cliquez sur **Paramètres de l'écran de veille** 5. Dans la nouvelle fenêtre qui s'affiche, cochez la case **A la reprise, demander l'ouverture de session** 6 afin de verrouiller l'ordinateur avec l'écran de veille et choisissez le délai d'inactivité avant l'activation de l'écran de veille 7. Enfin, validez et fermez la fenêtre en cliquant sur le bouton **OK** 8 :

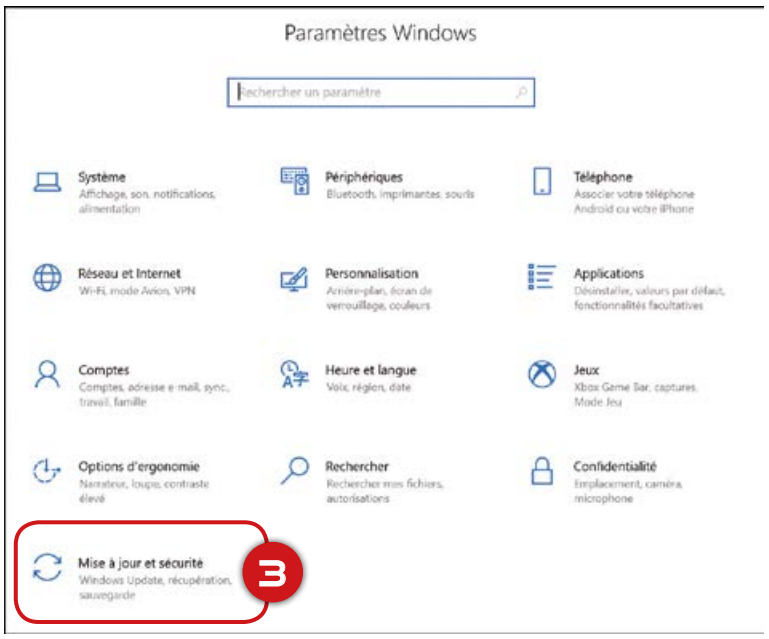


Désactiver la localisation

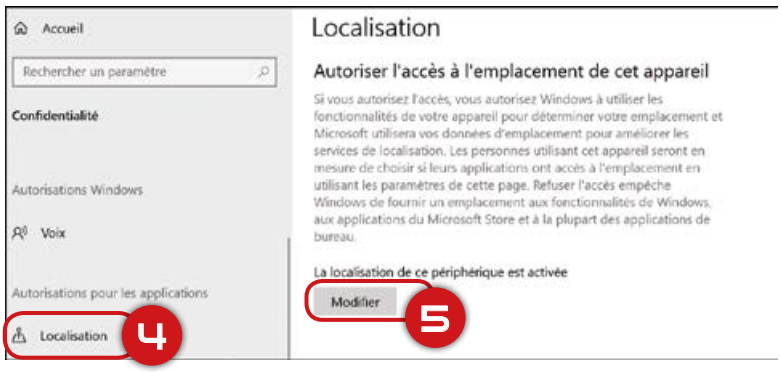
Pour désactiver l'accès complet à la localisation de votre appareil, vous devez être connecté à votre ordinateur avec un compte ayant des droits administrateurs.

Cliquez sur le bouton **Démarrer** ❶, ouvrez les **Paramètres** de Windows ❷, puis choisissiez le menu **Confidentialité** ❸ :





Dans la barre de menu latérale, descendez jusqu'au menu **Autorisation pour les applications**, choisissez **Localisation** ❹, puis cliquez sur le bouton **Modifier** ❺ :



Utilisez le bouton à bascule ❻ afin de désactiver la localisation de votre appareil :

Vous pouvez également autoriser l'accès à la localisation de votre appareil pour certaines applications seulement (voir le tutoriel « Restreindre les autorisations accordées aux applications »).

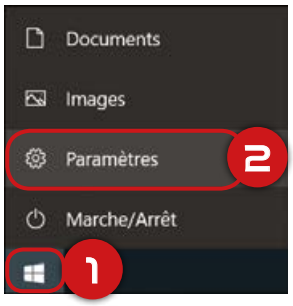
Notez que cette méthode a pour effet de polluer les journaux Windows à chaque tentative de démarrage du service. Pour les réseaux administrés, préférez plutôt la désactivation de la géolocalisation par stratégie de groupe (GPO). Pour cela, appuyez-vous sur le guide « **Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10** »[79] proposé par l'ANSSI.

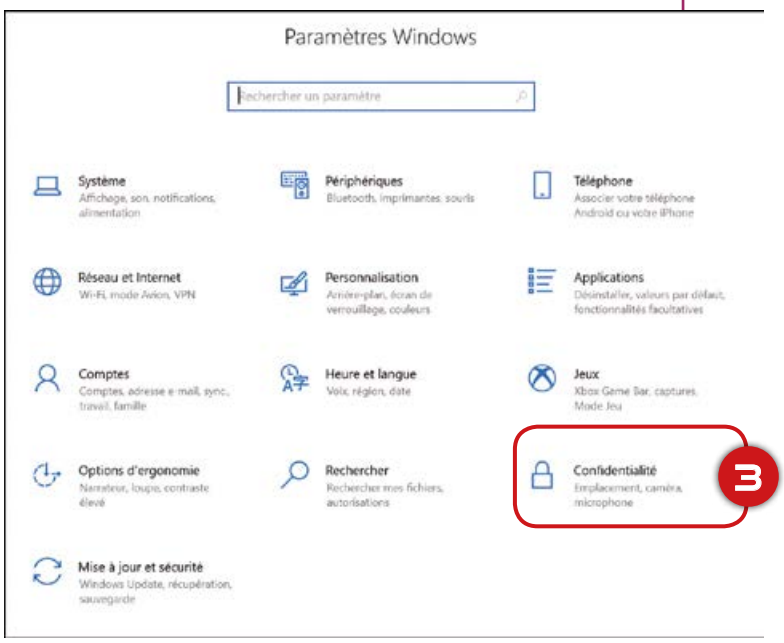
79 https://www.ssi.gouv.fr/uploads/2017/01/np_securisation_windows10_collecte_de_donnees_v1.2.pdf

Désactiver l'identifiant unique de publicité

Windows génère un identifiant de publicité unique pour chaque utilisateur d'un appareil, qui peut être utilisé par des réseaux publicitaires pour proposer de la publicité ciblée.

Afin de désactiver cet identifiant, cliquez sur le bouton **Démarrer** 1, ouvrez les **Paramètres** de Windows 2, puis choisissez le menu **Confidentialité** 3 :





Dans la barre de menu latérale, choisissez l'onglet **Général** 4, puis désactivez l'identifiant de publicité à l'aide d'un bouton à bascule 5 :

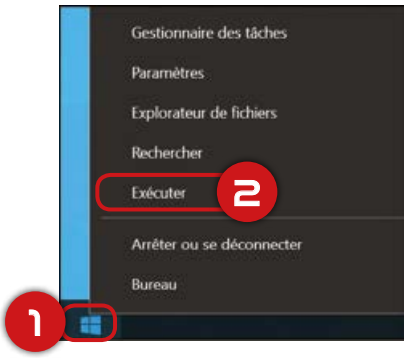
La désactivation de l'identifiant de publicité ne réduit pas le nombre de publicités affichées, mais sert à désactiver la publicité ciblée.

Désactiver Cortana

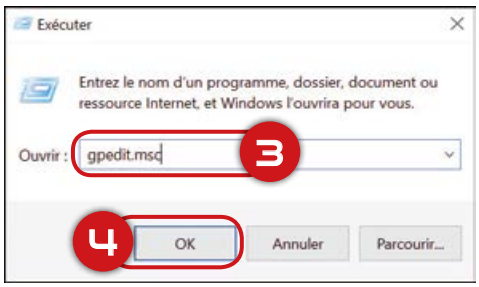
(+ Vidéo)

Attention, cette méthode concerne uniquement les versions **Professionnel** et **Entreprise** de Windows 10.

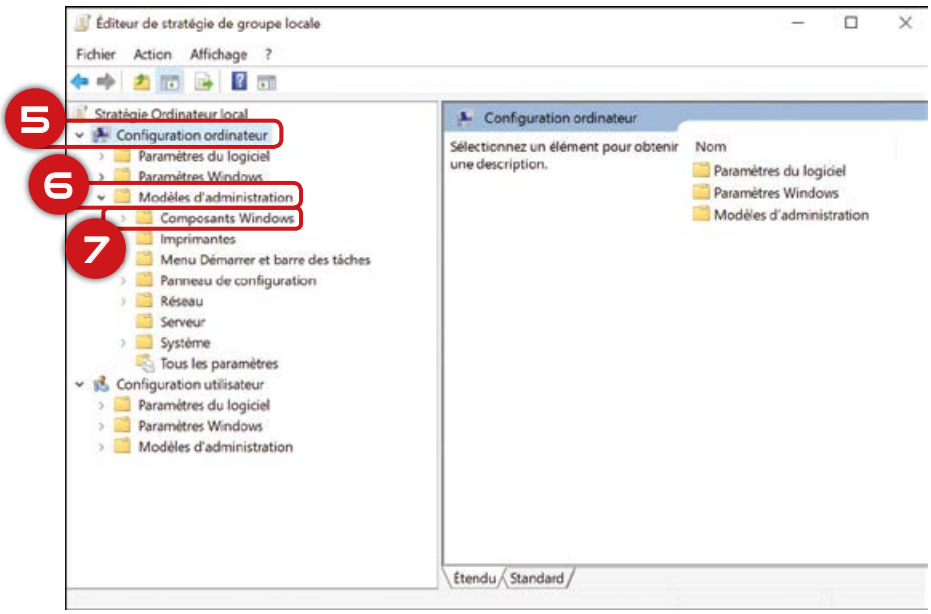
L'assistant virtuel de Microsoft appelé Cortana, récolte en permanence des informations sensibles sur vous qu'il peut divulguer à Microsoft, ses filiales et ses partenaires, notamment votre localisation géographique et vos emplacements habituels, votre historique de recherche, vos centres d'intérêt, vos contacts, vos rendez-vous, les informations de certaines applications (Santé), etc. Pour désactiver Cortana, vous devez être connecté à votre ordinateur à l'aide d'un compte ayant des droits administrateurs.



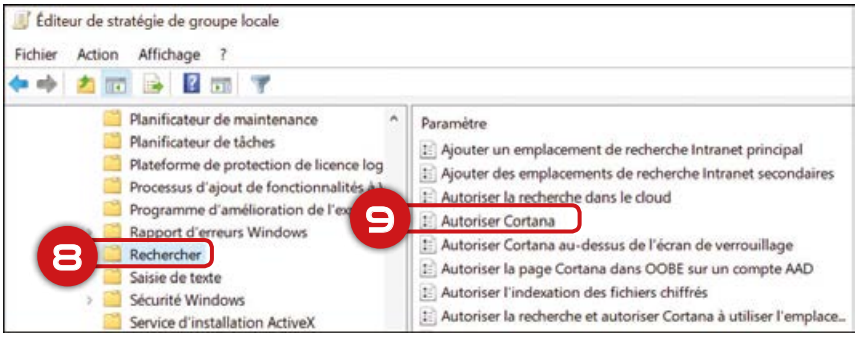
Faites un clic droit sur le bouton **Démarrer** ❶ et choisissez **Exécuter** ❷. Dans la nouvelle fenêtre qui s'ouvre, entrez **gpedit.msc** ❸ et cliquez sur le bouton **OK** ❹ :



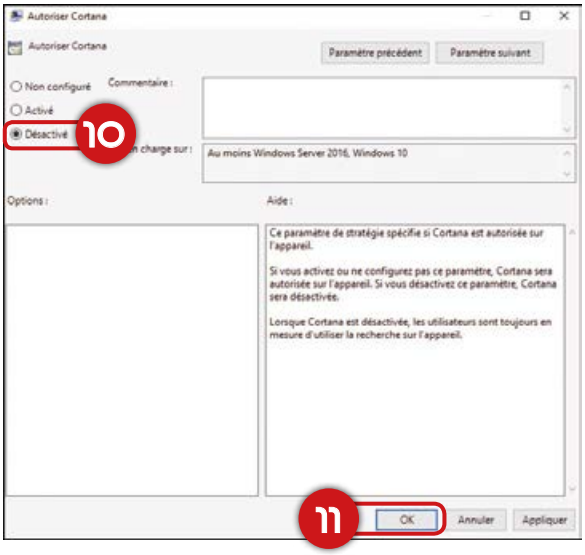
Ainsi, vous allez lancer l'outil d'administration, appelé l'éditeur de stratégie de groupe locale qui vous permet de configurer de nombreux paramètres dans Windows. Dans le menu **Configuration ordinateur** ❺ ouvrez le dossier **Modèles d'administration** ❻, puis **Composants Windows** ❼ :



Trouvez le dossier **Rechercher** 8, puis faites un double-clic sur le paramètre **Autoriser Cortana** 9 :



Une fenêtre des paramètres Cortana s'ouvre. Sélectionnez l'option **Désactivé** 10, puis validez votre choix à l'aide du bouton **OK** 11 :



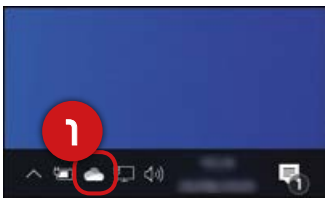
Fermez l'éditeur de stratégie de groupe locale. Déconnectez-vous de votre compte utilisateur puis reconnectez-vous (ou redémarrez votre ordinateur), afin que vos paramètres soient pris en compte.

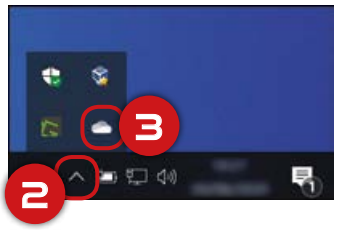
Désactiver OneDrive et supprimer les documents stockés en ligne

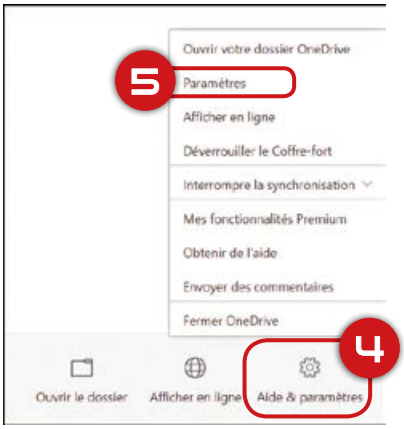
(+ Vidéo)

Renoncez à l'utilisation des services *Cloud* intégrés au système d'exploitation proposant des contrats standard dont vous ne maitrisez pas les clauses.

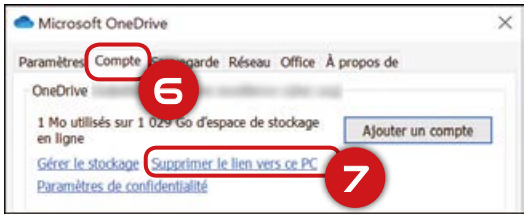
Recherchez l'icône de l'application OneDrive dans la barre des tâches ❶. Si l'icône n'est pas visible, sélectionnez **Afficher les icônes cachées** ❷, l'icône de OneDrive doit y être présente ❸ :



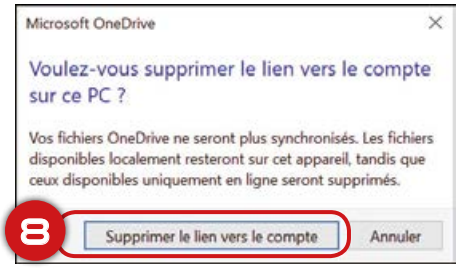




Faites un clic droit sur l'icône de OneDrive, choisissez le menu **Aide & paramètres** ❹, puis cliquez sur **Paramètres** ❺. Dans la nouvelle fenêtre qui s'ouvre, choisissez l'onglet **Compte** ❻, puis cliquez sur **Supprimer le lien vers ce PC** ❼ :



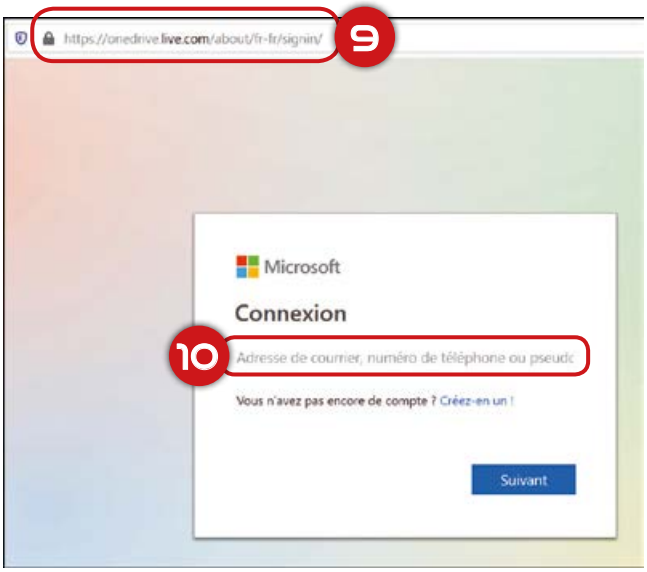
Une boîte de dialogue s'ouvre, vous devez alors confirmer votre choix ❽:



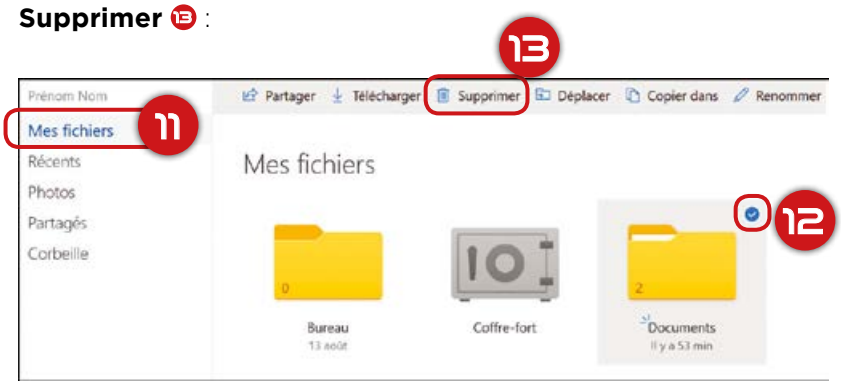
Après avoir désactivé OneDrive, désinstallez l'application de votre système si c'est possible[80] (voir le tutoriel « Désinstaller les applications »).

80 Il est possible de supprimer OneDrive sur certaines versions de Windows.

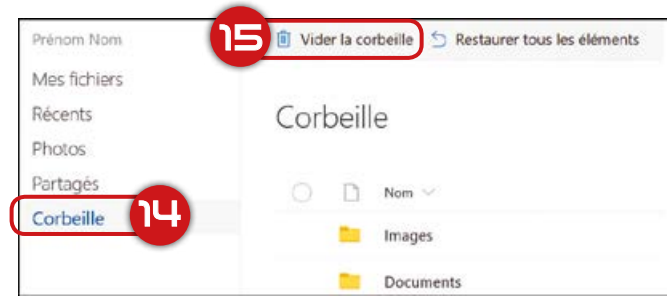
Le simple fait de désinstaller l'application **OneDrive** ou dissocier votre compte **OneDrive** de votre ordinateur n'entraîne pas de perte de vos fichiers ou documents. Vos données seront toujours présentes sur votre ordinateur et seront accessibles dans votre espace personnel en ligne de **OneDrive**. Pour supprimer toutes vos données stockées dans votre espace en ligne, connectez-vous sur le site de **OneDrive**[81] 9 à l'aide de votre compte Microsoft 10 :



Dans la barre de menu latérale, choisissez **Mes fichiers** 11, sélectionnez vos dossiers/fichiers que vous voulez supprimer 12, puis cliquez sur le bouton **Supprimer** 13 :



Avant de vous déconnecter, n'oubliez pas de vider la corbeille qui contient vos données supprimées. Pour cela, choisissez le menu **Corbeille** 14 dans la barre de menu latérale, puis cliquez sur le bouton **Vider la corbeille** 15 :



Notez que désactiver OneDrive désactive **l'enregistrement automatique des documents dans la suite Microsoft Office 365**.

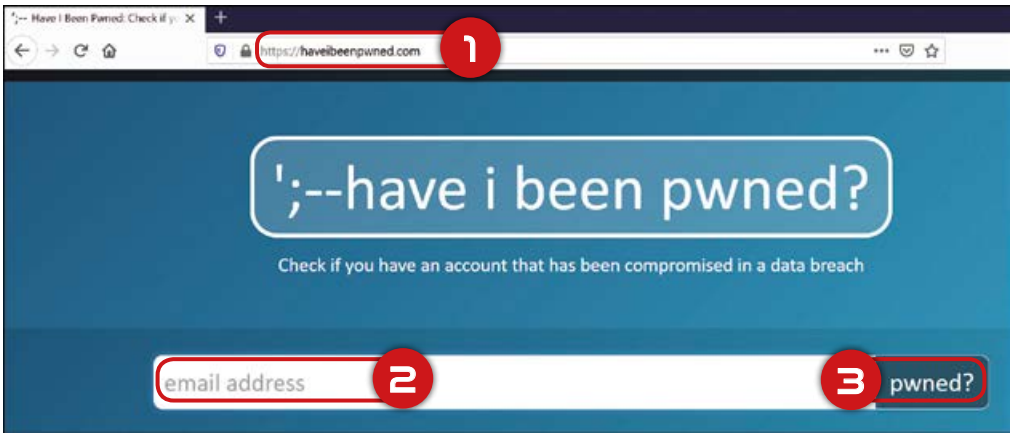
81 https://onedrive.live.com/about/fr-fr/signin/

Vérifier si une fuite de données en ligne vous concerne

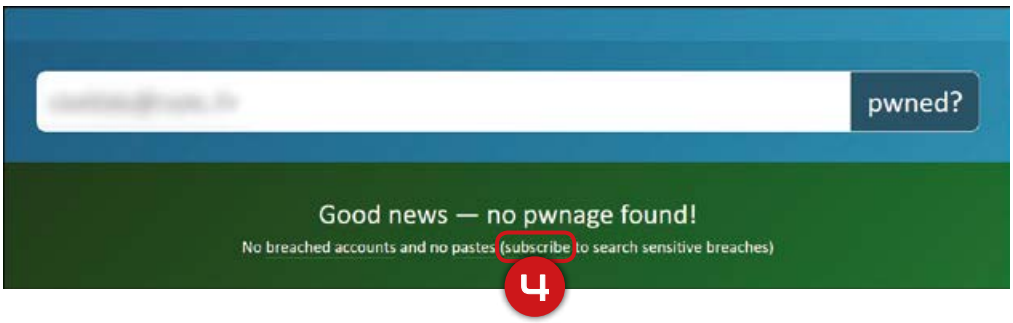
(+ Vidéo)

L'outil haveibeenpwened.com recensent les comptes de messageries électroniques qui ont été compromis à l'occasion de fuites massives de données. En entrant votre adresse électronique, vous pouvez savoir si elle figure dans l'une des bases de données piratées, quel site est à l'origine de la fuite, mais aussi si votre mot de passe ou d'autres données vous concernant sont potentiellement entre les mains de personnes malveillantes.

Ouvrez votre navigateur et allez sur le site https://haveibeenpwned.com[82] 1. Saisissez l'adresse électronique que vous voulez vérifier 2, puis cliquez sur le bouton « **pwned?** » 3 :



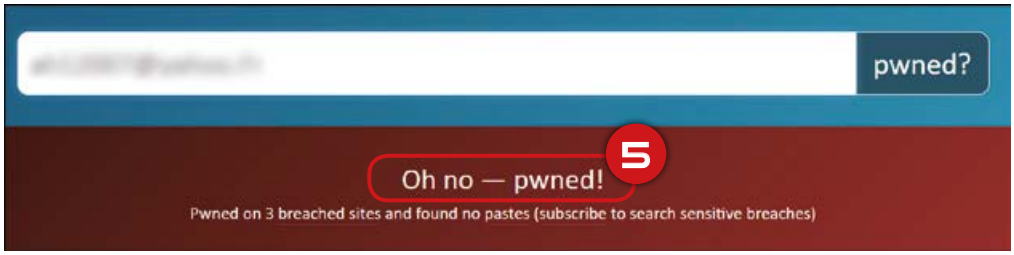
Si votre adresse n'apparait dans aucune base de données connue, vous allez voir le message « Good news – no pwnage found! ». Vous avez toutefois la possibilité de vous inscrire au service de notification qui vous enverra un message automatique dès lors que votre adresse électronique se retrouve dans une fuite de données (site piraté, base de données exposée, etc.). Pour cela, cliquez sur le bouton **subscribe** 4 :



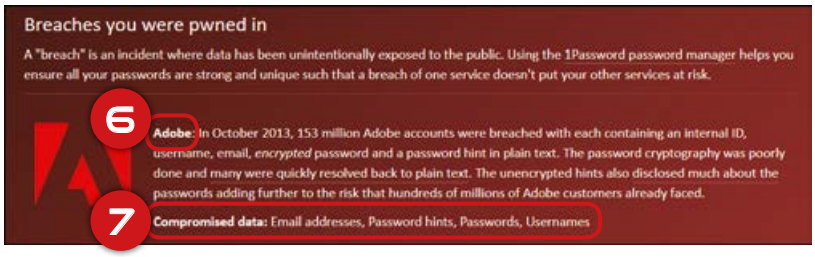
C'est un service gratuit et vous pouvez vous désabonner à tout moment si vous ne souhaitez plus recevoir les notifications.

82 « have i been pwned? » = « Est-ce que je me suis fait avoir ? »

Si l'un de vos comptes en ligne a été exposé à une fuite de données connue, vous allez voir le message « Oh no – pwned! » 5 :



L'outil vous renvoi alors les noms des sites Web 6 qui ont été victimes de piratage et sur lesquels vous vous êtes inscrit avec votre adresse électronique, ainsi que la nature des données potentiellement compromises 7 :



Vous devez alors rapidement changer vos mots de passe des comptes potentiellement compromis.

Une alternative en français au site Web https://haveibeenpwned.com est Firefox Monitor (https://monitor.firefox.com/).

Gestion des mots de passe avec KeePass

(+ 3 Vidéos)

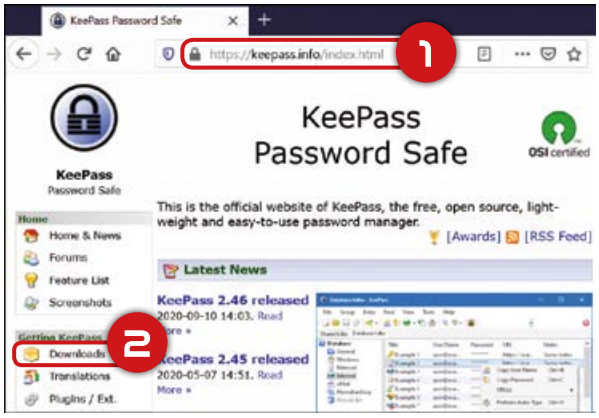
KeePass est un gestionnaire de mots de passe gratuit et open source, qui vous aide à gérer vos mots de passe de manière sécurisée. Vous pouvez stocker tous vos mots de passe dans une base de données (un fichier chiffré), qui est protégée par un mot de passe principal. Il vous suffit donc de vous souvenir d'un seul mot de passe pour déverrouiller l'ensemble de la base de données.

Ce tutoriel est divisé en quartes étapes :
Téléchargement, Installation, Configuration de la langue et Utilisation.

Téléchargement

Il existe un grand nombre de faux sites qui vous proposent de télécharger des versions corrompues de KeePass. Faites donc bien attention et ne téléchargez KeePass que sur le seul site officiel de l'éditeur www.keepass.info ❶.

Sur la page d'accueil du site, dans le menu latéral, cliquez sur **Downloads** ❷ :



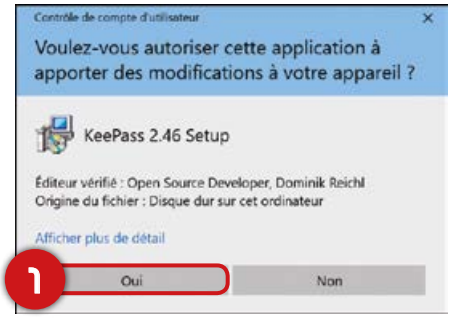
Lancez le téléchargement de la dernière version exécutable du logiciel en cliquant sur le bouton **Download Now** ❸ :

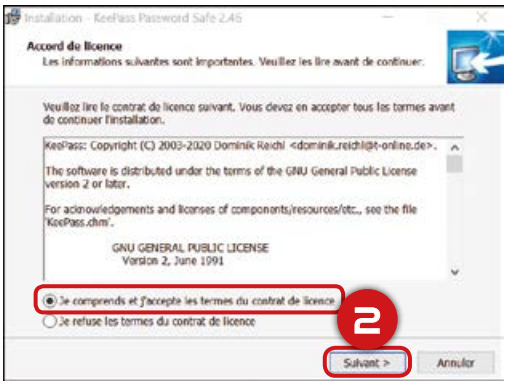
Vous allez être redirigé vers le site sourceforge.net à partir duquel le téléchargement se lance de manière automatique. Lorsqu'une fenêtre s'ouvre, cliquez sur **Enregistrer le ficher** ❹ :

Après avoir téléchargé le fichier exécutable, analysez-le avec votre anti-virus ou à l'aide de VirusTotal (voir le tutoriel « Analyser un fichier ou un lien avec VirusTotal »). Vous pouvez lancer l'installation du logiciel seulement si le fichier exécutable est sain.

Installation

Faites un double clic sur le fichier exécutable. Vous allez devoir entrer votre mot de passe administrateur ou confirmer votre choix ❶. L'assistant d'installation se lance, afin de poursuivre l'installation vous allez devoir acceptez les termes du contrat de licence ❷ :

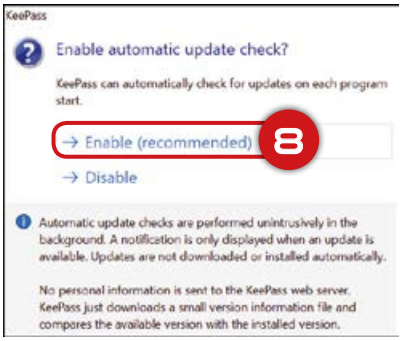




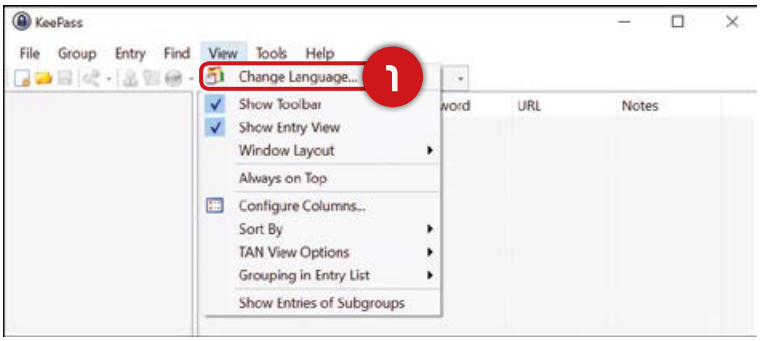
Laissez le dossier de destination ainsi que les composants à installer par défaut et cliquez sur **Suivant** ❸ ❹ :

Cochez les cases permettant de créer des icônes supplémentaires ❺ et cliquez sur **Suivant** ❻ :

Enfin, cliquez sur le bouton **Installer** 7 et acceptez les mises à jour automatiques 8 :



Configuration de la langue

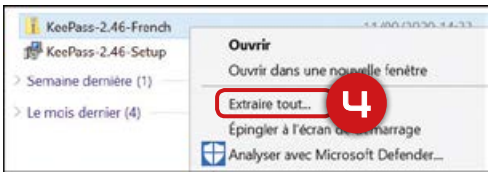


Par défaut, l'interface de KeePass est en anglais. Les étapes suivantes vous guideront afin de configurer son interface en français. Ouvrez l'application KeePass, choisissez l'onglet **View** et cliquez sur **Change Language** 1 :

Dans la nouvelle fenêtre qui s'ouvre, cliquez sur **Get More Languages** 2, votre navigateur va ouvrir automatiquement le site de KeePass :

Sur la page Web, trouvez la langue française dans le tableau, téléchargez la version la plus récente du paquet linguistique 3 et analysez le fichier téléchargé :

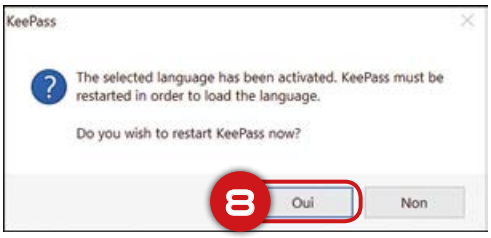
Allez dans le dossier où se trouve le paquet linguistique que vous venez de télécharger. Pour le décompresser, faites un clic droit et choisissez **Extraire tout** 4 :



Laissez la fenêtre qui s'ouvre contenant le fichier linguistique 5 ouverte :

Dans KeePass, ouvrez à nouveau le menu **View** -> **Change Languages** et choisissez **Open Folder** 6. Un dossier vide s'ouvre automatiquement, copiez le fichier linguistique de l'étape 5 et collez-le dans ce dossier. Vous allez devoir rentrer votre mot de passe administrateur. Dans KeePass, ouvrez à nouveau le menu **View** -> **Change Languages** et choisissez la langue française 7 :

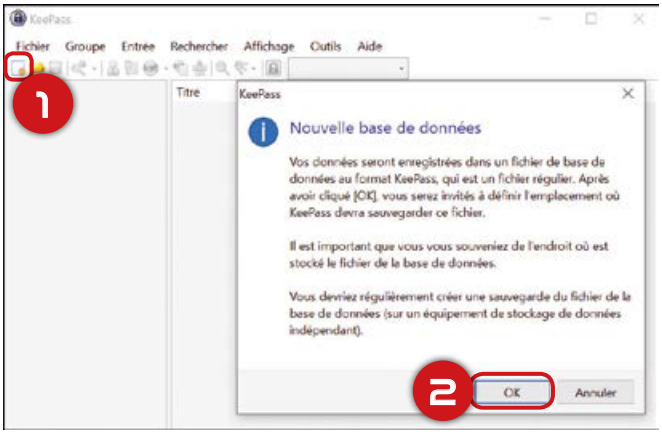
Une fenêtre de dialogues vous invite à redémarrer KeePass, acceptez-le en cliquant sur le bouton Oui 8 :



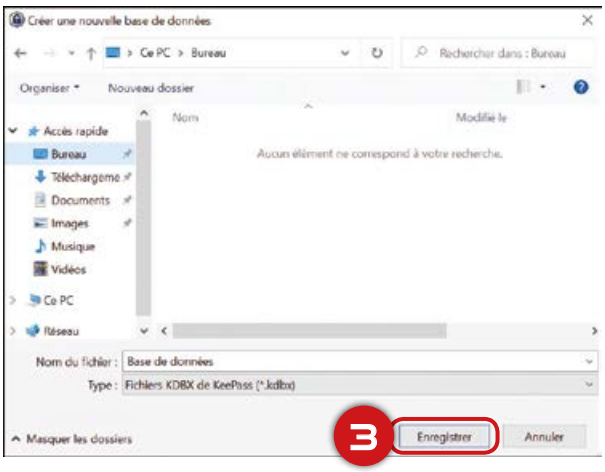
Après redémarrage, l'application va prendre en charge la nouvelle langue.

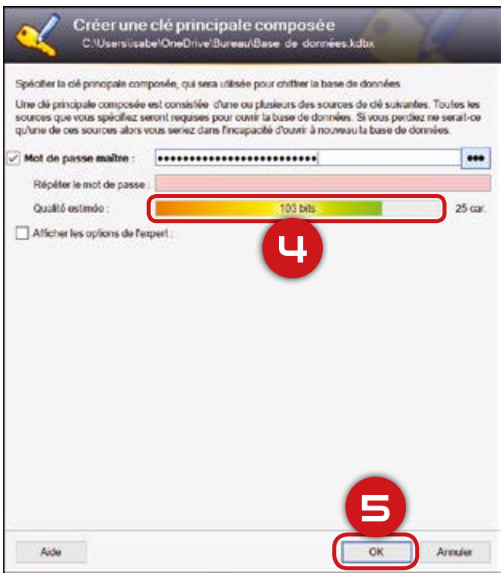
Utilisation

Lors de la première utilisation, il est nécessaire de créer une base de données qui va regrouper tous vos mots de passe dans un seul fichier. Pour cela, cliquez sur l'icône en haut à gauche ❶, puis sur le bouton **OK** ❷ :



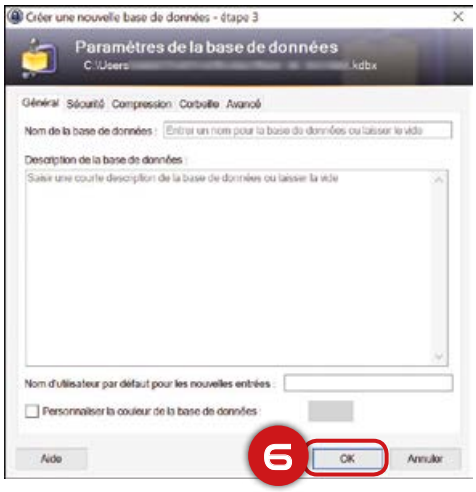
Choisissez l'emplacement et le nom de votre base (évitez les noms qui permettent de savoir qu'il s'agit d'une base contenant les mots de passe), puis cliquez sur **Enregistrer** ❸. Une nouvelle fenêtre s'ouvre, qui vous invite à créer le mot de passe principal. C'est le seul mot de passe que vous devez retenir, car il vous permettra d'accéder à tous vos mots de passe. L'indicateur de complexité du mot de passe permet d'évaluer le risque de sécurité[83]. Plus l'indicateur tend vers le vert, plus le mot de passe est robuste ❹. Une fois le mot de passe choisi, cliquez sur **OK** ❺ :

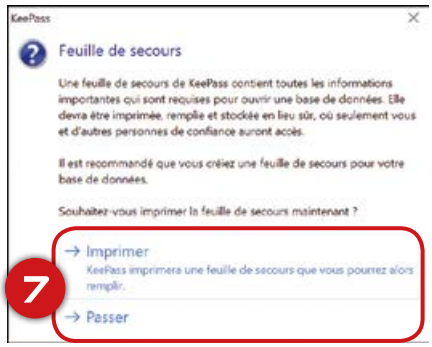




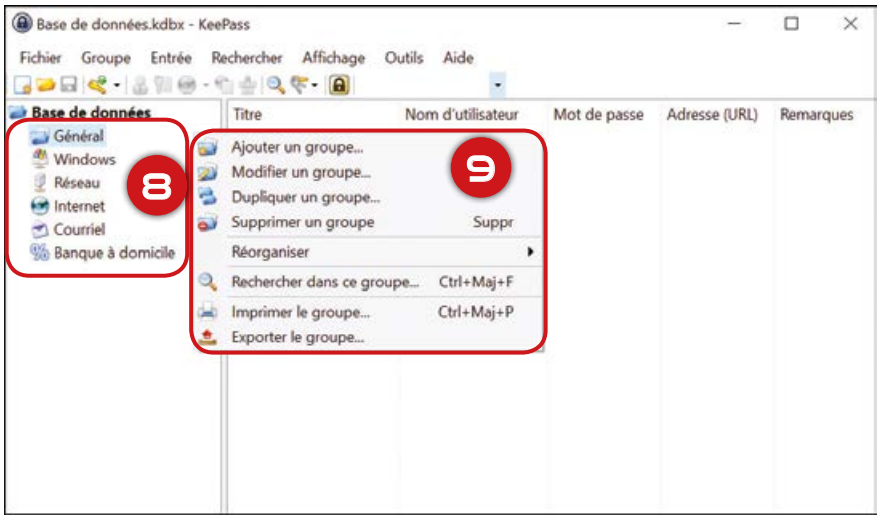
83 Suivez les conseils de la fiche « Mots de passe ».

Les deux étapes suivantes sont facultatives. Tout d'abord, vous pouvez affiner les paramètres de la base (ajouter une description, modifier les algorithmes de chiffrements, etc.). Vous pouvez passer cette étape en cliquant simplement sur le bouton **OK** 6. Enfin, l'outil vous propose d'imprimer et remplir une feuille de secours 7 qui contient toutes les informations importantes qui sont requises pour ouvrir votre base de données. Cliquez sur **Imprimer** ou **Passer** 7 :



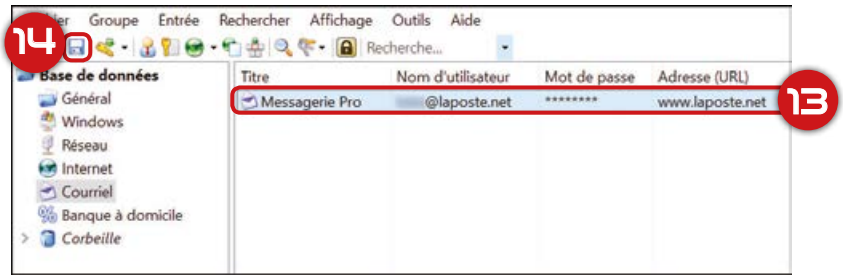


Une fois la base de données créée, l'outil crée plusieurs groupes par défaut (Général, Windows, Courriel, etc.) qui s'affichent à gauche 8 et qui permettent de séparer les mots de passe par catégorie. Vous pouvez ajouter de nouveaux groupes ou modifier les groupes existants en faisant un clic droit 9 :



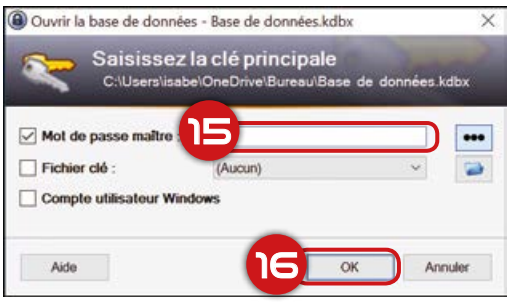
Pour ajouter une nouvelle entrée de mot de passe, il suffit de cliquer sur le groupe désiré, puis sur l'icône avec une clé et une flèche verte ⑩. Une nouvelle fenêtre s'ouvre qui vous permet de renseigner le titre de la nouvelle entrée (par exemple, Messagerie Pro), le nom d'utilisateur (le login), l'adresse URL, l'expiration du mot de passe, sa complexité, etc. Pour chaque nouvelle entrée, un mot de passe est généré de manière automatique. Vous pouvez le garder ou le modifier. Vous pouvez visualiser votre mot de passe en cliquant sur les trois points ⑪.

Après avoir validé la nouvelle entrée ⑫, elle apparait dans la partie droite de KeePass ⑬. Lorsque vous faites un double-clic sur le titre de l'entrée, vous avez la possibilité de la modifier. Lorsque vous faites un double-clic sur l'adresse URL, le site correspondant s'ouvre automatiquement dans votre navigateur. Pour copier rapidement le nom d'utilisateur ou le mot de passe, faite un double-clic dessus. Vous pouvez alors les coller dans les champs correspondants afin de vous connecter à votre compte. Pour des raisons de sécurité, les informations copiées ne sont gardées en mémoire que pendant un temps donné (12 secondes par défaut).

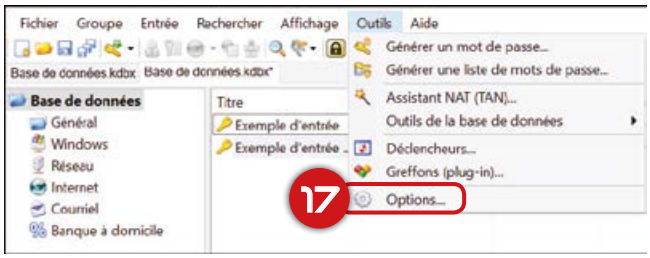


Avant de quitter l'outil, n'oubliez pas d'enregistrer la base, afin que les modifications effectuées ne soient pas perdues. Pour cela, il suffit de cliquer sur l'icône ⑭.

Lors du prochain lancement de KeePass, le mot de passe principal vous sera demandé. Après l'avoir saisi 15 puis validé par **OK** 16, la base sera à nouveau accessible.



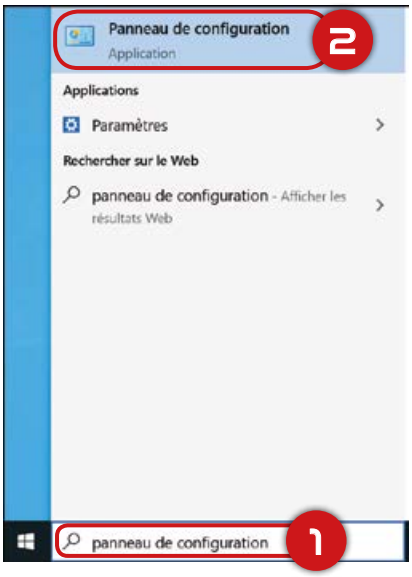
Vous avez la possibilité de paramétrer l'outil en allant dans le menu Outils, puis Options 17. Toutefois, nous vous conseillons de laisser les valeurs par défaut.



Créer un disque de réinitialisation de mot de passe pour un compte local

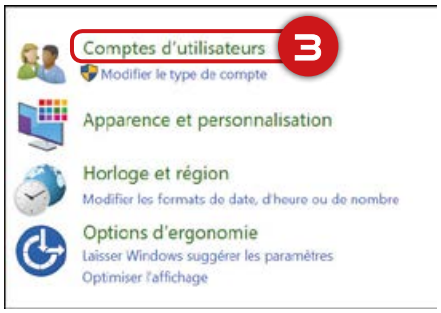
(+ Vidéo)

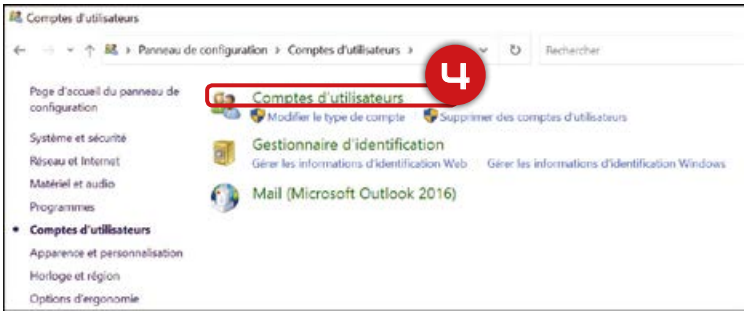
Lorsque vous utilisez un compte local[84] dans Windows 10, vous avez la possibilité de créer un disque de réinitialisation de mot de passe à l'aide d'une clé USB qui vous permettra de réinitialiser votre mot de passe en cas d'oubli. Nous vous conseillons de créer cet outil dès que possible, n'attendez pas d'avoir oublié votre mot de passe, car il sera trop tard.



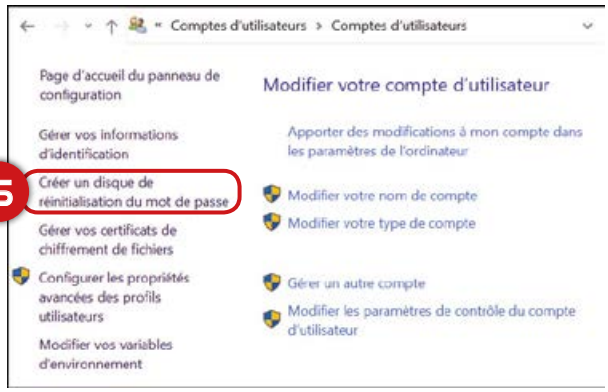
Tout d'abord, connectez à votre ordinateur une clé USB vide. Dans la zone de recherche[85] sur la barre des tâches, saisissez «**panneau de configuration**» ❶, puis ouvrez le **Panneau de configuration** ❷ :

Dans le panneau de configuration, choisissez **Comptes d'utilisateurs** ❸, puis cliquez à nouveau sur **Comptes d'utilisateurs** ❹ :



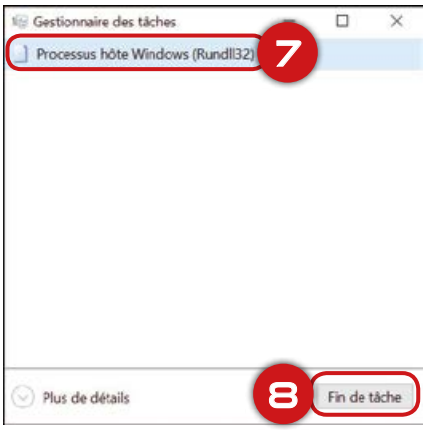


Dans la barre de menu latérale, choisissez **Créer un disque de réinitialisation du mot de passe** ❺ :



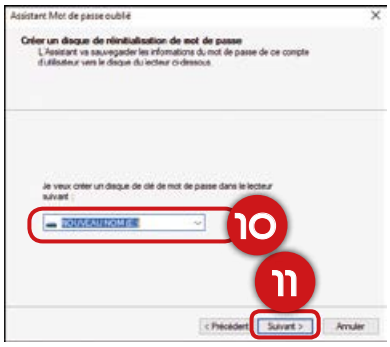
84 Cette méthode ne s'applique pas aux comptes Microsoft, car le mot de passe d'un compte Microsoft n'est pas stockés sur votre ordinateur, mais sur un serveur distant.
85 Si la zone de recherche est invisible, regarder le tutoriel «Afficher les extensions des fichiers».

Pour certains utilisateurs, si rien ne se passe, faites un clic droit sur la barre des tâches et choisissez **Gestionnaire des tâches** 6. Dans la nouvelle fenêtre qui s'ouvre, sélectionnez le **Processus hôte Windows (Rundll32)** 7 et cliquez sur **Fin de tâche** 8 :



Il s'agit d'un utilitaire Windows pouvant interférer avec l'outil de réinitialisation de mot de passe.

Cliquez à nouveau sur **Créer un disque de réinitialisation du mot de passe** 5. L'outil « Assistant de mot de passe oublié » va se lancer, cliquez sur **Suivant** 9, choisissez votre clé USB dans la liste déroulante 10 et continuez 11 :



À l'étape suivante, vous êtes invité à entrer le mot de passe du compte d'utilisateur actuel 12. Cliquez sur **Suivant** 13, attendez que la barre d'état atteigne 100%, puis continuez 14 :

À la fin du processus, cliquez sur le bouton **Terminer** 15 :

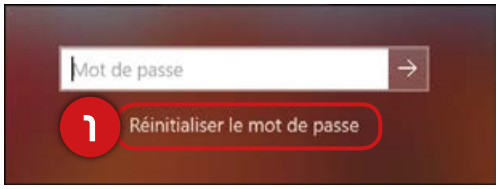
Retirez la clé USB et conservez-la dans un lieu sûr dont vous vous souviendrez. Notez qu'il n'est pas nécessaire de créer un nouveau disque lorsque vous modifiez votre mot de passe et ce, même à plusieurs reprises.

Réinitialiser le mot de passe oublié d'un compte local

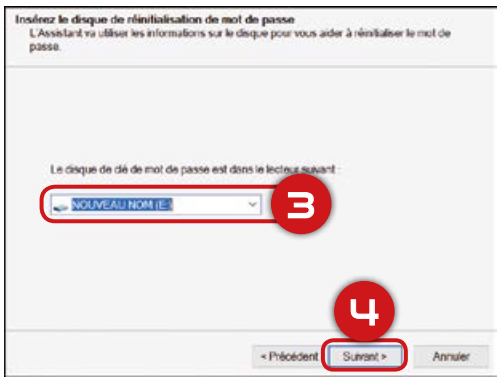
(+ Vidéo)

Si vous avez oublié le mot de passe de votre compte local, vous pouvez facilement définir un nouveau mot de passe à l'aide du disque de réinitialisation que vous avez créé au préalable (voir le tutoriel « Créer un disque de réinitialisation de mot de passe pour un compte local »).

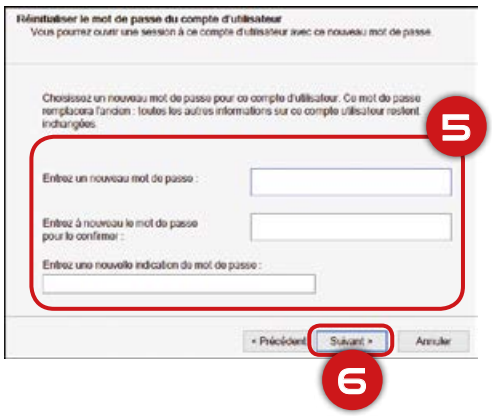
Lorsque vous essayez de vous connecter à votre compte en entrant un mauvais mot de passe, le système vous propose de le réinitialiser. Connectez à votre ordinateur votre disque de réinitialisation de mot de passe (clé USB), puis cliquez sur le lien **Réinitialiser le mot de passe** ❶ :



Un assistant de réinitialisation du mot de passe s'ouvre. Cliquez sur le bouton **Suivant** ❷, choisissez votre clé dans la liste déroulante ❸, puis continuez ❹ :



À l'étape suivante, choisissez un nouveau mot de passe pour le compte courant ❺ et cliquez sur le bouton **Suivant** ❻. Enfin, pour fermer l'assistant, cliquez sur le bouton **Terminer** ❼ :

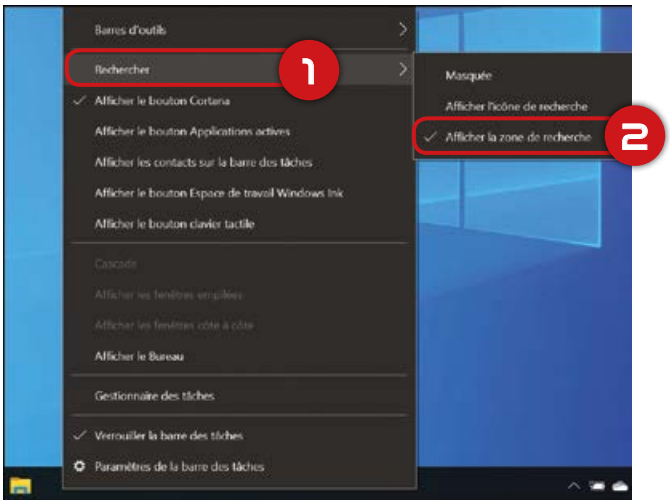


Retirez la clé USB et connectez-vous à votre compte à l'aide de votre nouveau mot de passe.

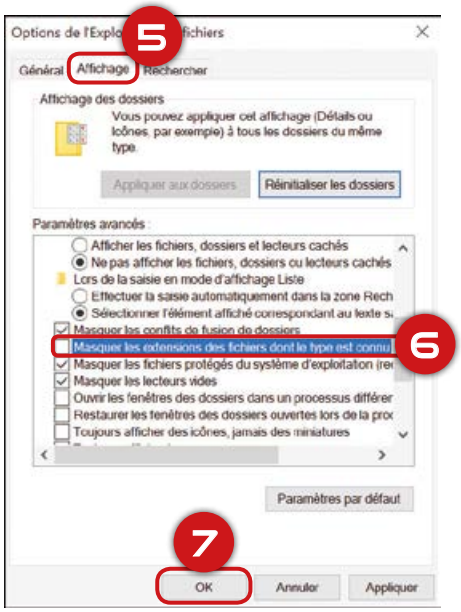
Afficher les extensions des fichiers

L'absence d'extension peut tromper sur la véritable nature d'un fichier, par exemple, un fichier image peut en réalité être un exécutable contenant un programme malveillant. Il suffit pour cela de nommer un fichier image.jpg.exe : si l'extension .exe est masquée, vous ne verrez que image.jpg en pensant qu'il s'agit juste d'une image[86]. Lorsque vous allez l'ouvrir, c'est l'exécution du code malveillant que vous allez lancer.

Afin d'activer l'affichage des extensions des fichiers, vous avez besoin d'utiliser la zone de recherche Windows. Si votre zone de recherche ne s'affiche pas correctement ou est masquée[87], cliquez avec le bouton droit sur la barre des tâches, puis sélectionnez **Rechercher** ❶ et **Afficher la zone de recherche** ❷ :



Dans la zone de recherche Windows saisissez « options de l'explorateur de fichiers » ❸, puis lancez l'outil trouvé ❹. Dans la fenêtre qui s'ouvre, choisissez l'onglet **Affichage** ❺. En déroulant la liste, trouvez et décochez la case de l'option **Masquer les extensions des fichiers dont le type est connu** ❻, puis cliquez sur le bouton **OK** ❼ :



86 https://www.commentcamarche.net/informatique/windows/185-afficher-les-extensions-et-les-fichiers-caches-sous-windows/
87 https://support.microsoft.com/fr-fr/help/4028221/windows-10-locating-the-search-box-in-windows-10

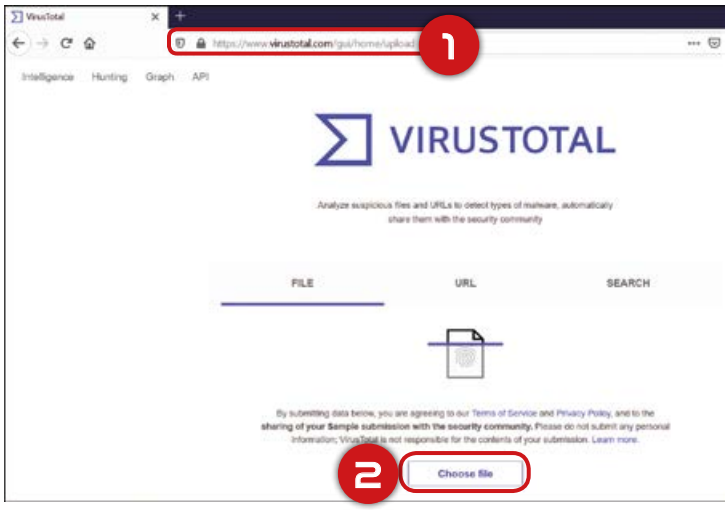
Analyser un fichier ou un lien avec VirusTotal

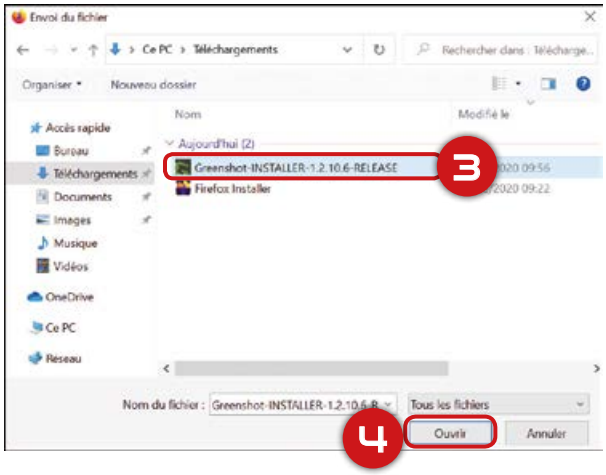
(+ Vidéo)

VirusTotal un outil en ligne gratuit qui permet d'analyser un fichier ou un lien URL avec plusieurs antivirus afin de déterminer si cet élément est corrompu ou sain.

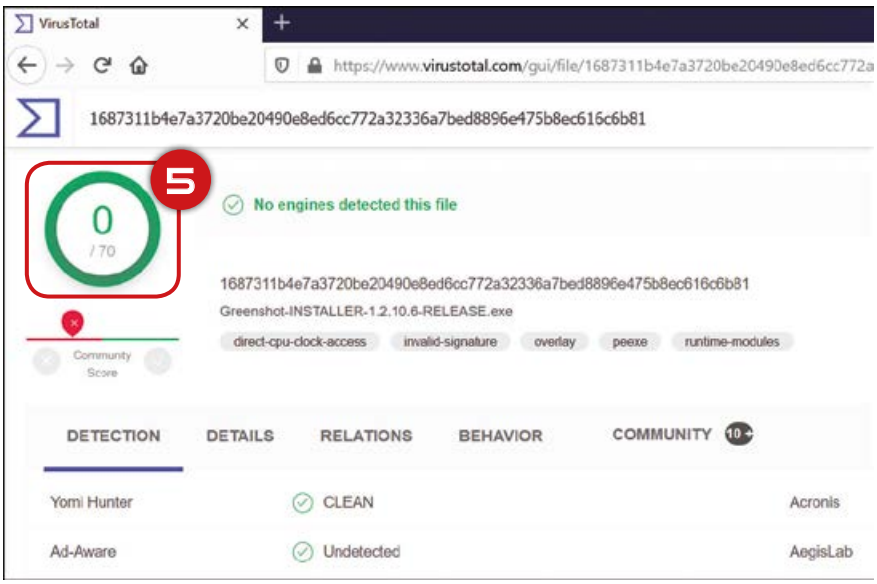
Ouvrez votre navigateur et allez sur le site www.virustotal.com ❶.

Pour analyser un fichier, cliquez sur le bouton **Choose file** ❷, naviguez dans l'explorateur de fichiers qui s'ouvre afin de sélectionner le fichier que vous voulez analyser ❸, puis cliquez sur le bouton **Ouvrir** ❹ :

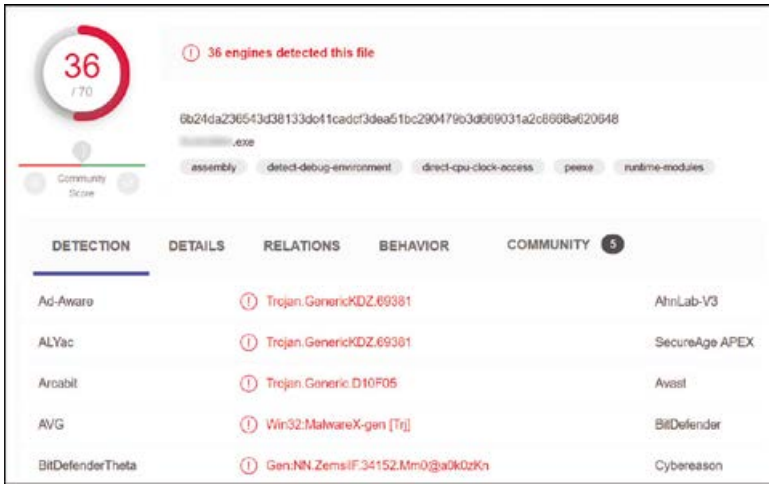




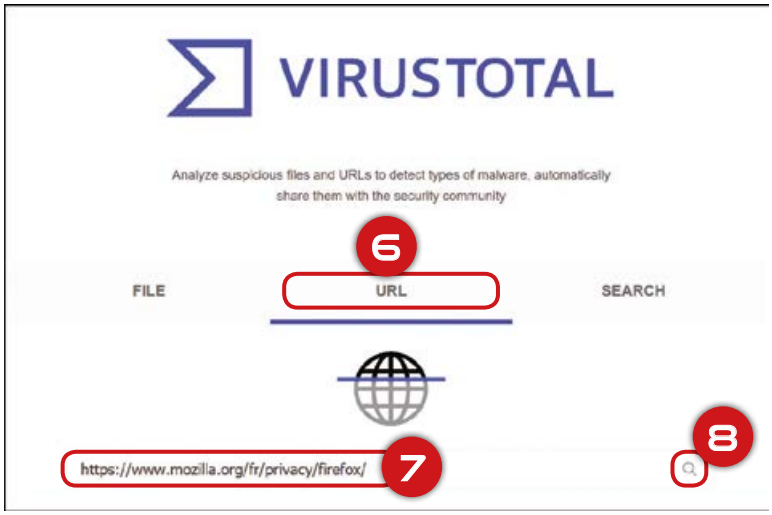
Le fichier va être analysé par plusieurs anti-virus en même temps. Le résultat d'analyse est représenté par un cercle avec le pourcentage de détection ❺. Lorsque le cercle est vert, le fichier est considéré comme sain.



Ci-dessous, un exemple d'analyse d'un fichier infecté, 36 anti-virus détectent un malware dans le fichier analysé :



Pour analyser un lien, choisissez l'onglet **URL** 6 sur la page principale de l'outil. Collez le lien que vous voulez analyser dans le champ (attention de copier l'adresse du lien et de ne pas la confondre avec l'adresse) 7, puis cliquez sur le bouton en forme de loupe 8 :



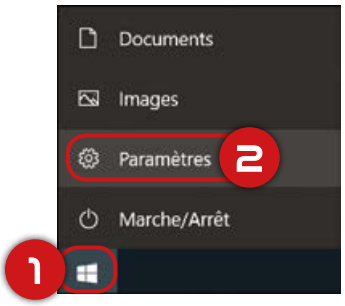
Les résultats d'analyse se présentent sous la même forme que pour les analyses de fichiers.

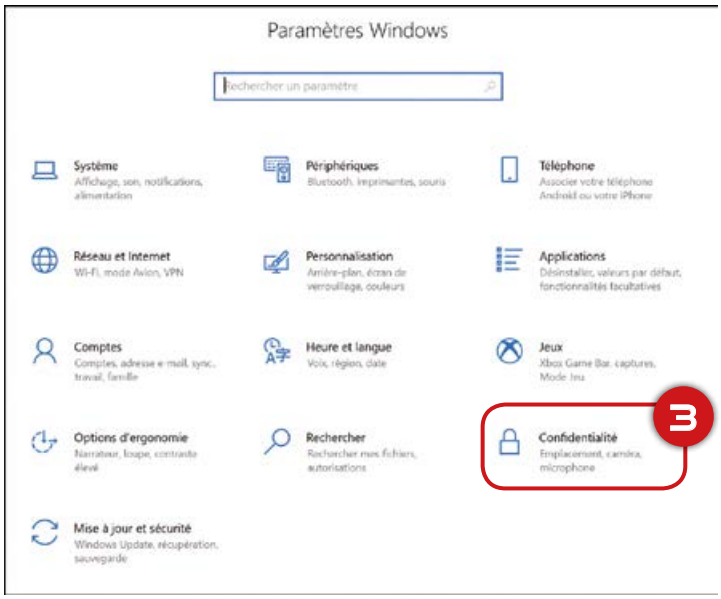
Attention : **ne soyez pas trop curieux**, car **le simple fait de positionnez le curseur de votre souris sur un lien** (sans cliquer) pour afficher l'adresse vers laquelle il pointe réellement (un autre lien vers un site frauduleux peut apparaitre alors) **peut déclencher le téléchargement intempestif d'un virus** !

Restreindre les autorisations accordées aux applications

Les applications peuvent accéder à des ressources potentiellement sensibles de votre système, comme la géolocalisation, la caméra, le microphone, les carnets d'adresse, etc. Vous pouvez régler les autorisations accordées aux applications pour certains paramètres de votre système.

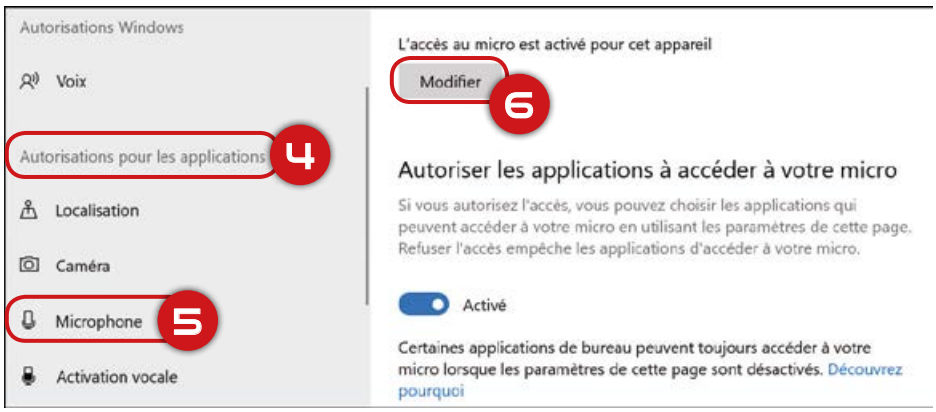
Pour cela, cliquer sur le bouton **Démarrer** 1, ouvrez les **Paramètres** de Windows 2, puis choisissiez le menu **Confidentialité** 3 :





Dans la barre de menu latérale, descendez jusqu'au menu **Autorisation pour les applications** 4. Choisissez le paramètre que vous voulez configurer, par exemple l'accès au **Microphone** 5. Plusieurs possibilités de configuration existent et cela pour chaque paramètre. Par exemple :

- Vous pouvez bloquer l'accès complet au microphone pour les applications et fonctionnalités Windows de tous les comptes utilisateur de votre appareil simultanément : dans ce cas, vous devez être connecté avec un compte administrateur. Cliquez sur le bouton **Modifier** 6 sous la phrase L'accès au micro est activé pour cet appareil :



Une petite fenêtre s'ouvre, utilisez le bouton à bascule pour désactiver l'accès complet au microphone 7 :

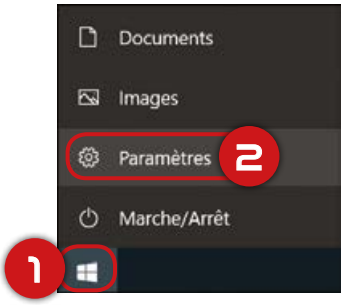
- Vous pouvez bloquer l'accès au microphone pour toutes les applications de votre compte utilisateur personnel : utilisez le bouton à bascule 8 dans la zone « Autoriser les applications à accéder à votre micro » :

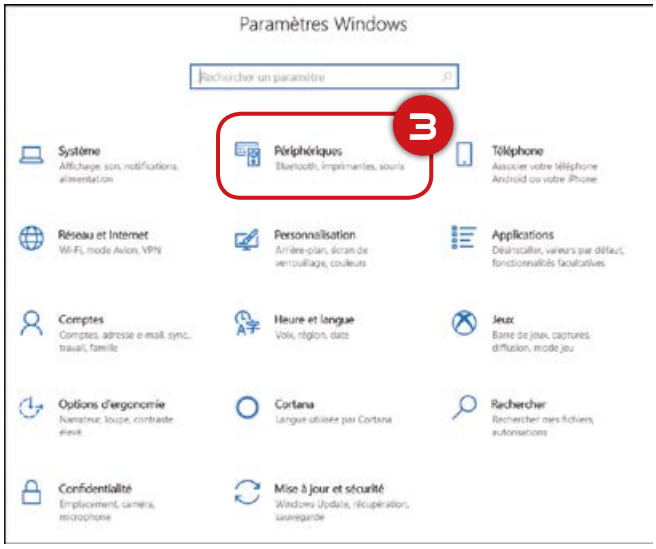
- Enfin, vous pouvez définir manuellement les applications de votre compte utilisateur personnel qui seront autorisées à utiliser le microphone : activez ou désactivez l'accès au microphone pour chaque application installée en utilisant les boutons à bascule correspondants 9 :

Désactiver l'exécution automatique à partir des supports amovibles

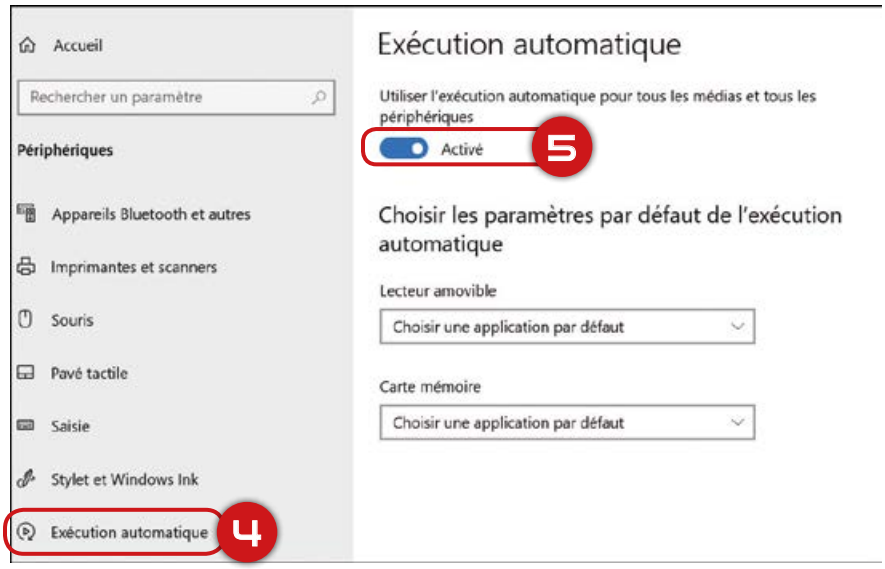
La désactivation de **l'exécution automatique** est une bonne pratique qui permet **d'empêcher l'exécution d'applications** de manière automatique lors de la connexion d'une clé USB ou d'un disque dur externe.

Cliquez sur **Démarrer** ❶, puis sur **Paramètres** ❷. Dans la fenêtre **Paramètres Windows** qui s'affiche choisissez **Périphériques** ❸ :

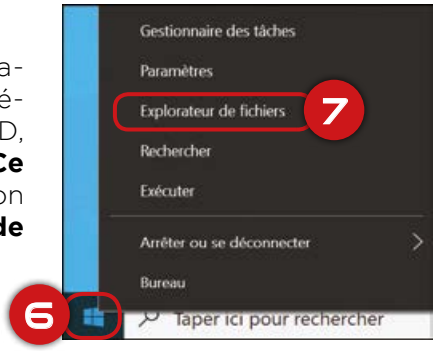




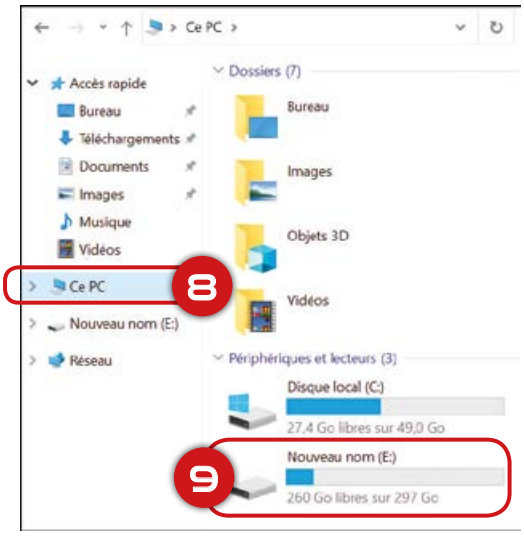
Dans la barre de menu latérale choisissez **Exécution automatique** ❹, puis désactivez cette fonction à l'aide d'un bouton à bascule ❺ :



Après avoir désactivé l'exécution automatique, vous pourrez accéder à vos périphériques amovibles (clé USB, carte SD, CD/DVD, disque dur externe) à l'aide de l'application **Ce PC**. Pour cela, faites un clic droit sur le bouton **Démarrer** 6, puis choisissez **Explorateur de fichiers** 7 :



Dans l'explorateur de fichiers qui s'ouvre, cliquez sur **Ce PC** 8, sélectionnez le périphérique amovible connecté à votre ordinateur 9 et faites un double clic afin de l'ouvrir :



Mettre en place un conteneur chiffré VeraCrypt

(+ 2 Vidéos)

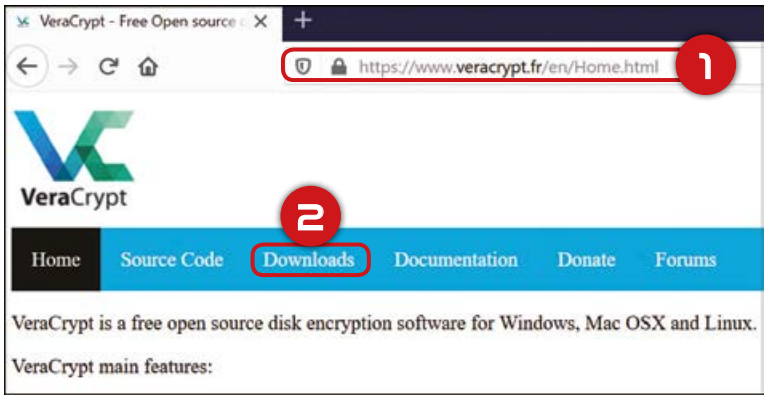
VeraCrypt est un logiciel libre et gratuit de chiffrement de disque pour des systèmes Windows, Mac OS et Linux. Cet outil permet, entre autres, de créer un fichier conteneur chiffré dans lequel vous pouvez déposer les données que vous voulez protéger. VeraCrypt permet également de chiffrer tout ou une partie d'un disque dur externe ou interne, ainsi qu'une clé USB.

Ce tutoriel est divisé en quatre étapes : Téléchargement, Installation, Créer un fichier conteneur chiffré et Utiliser le fichier conteneur chiffré.

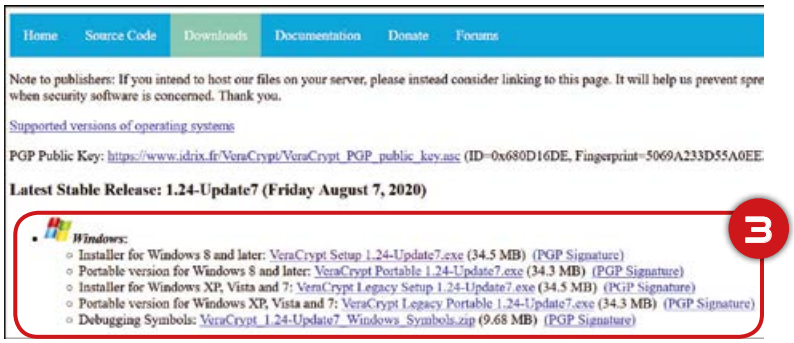
Téléchargement

Téléchargez VeraCrypt sur le site officiel de l'éditeur www.veracrypt.fr 1.

Sur la page d'accueil du site cliquez sur l'onglet **Downloads** 2 :



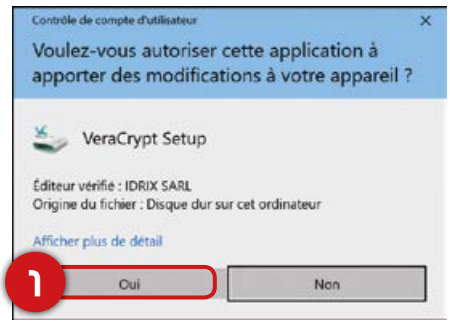
Choisissez la version qui correspond à votre système d'exploitation et lancez le téléchargement en cliquant sur l'exécutable 3 :



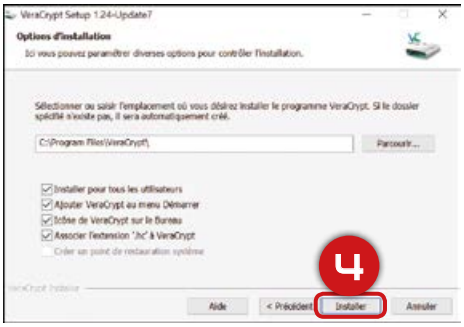
Après avoir téléchargé le fichier exécutable, analysez-le avec votre anti-virus ou à l'aide de VirusTotal (voir le tutoriel « Analyser un fichier ou un lien avec VirusTotal »). Vous pouvez lancer l'installation du logiciel seulement si le fichier exécutable est sain.

Installation

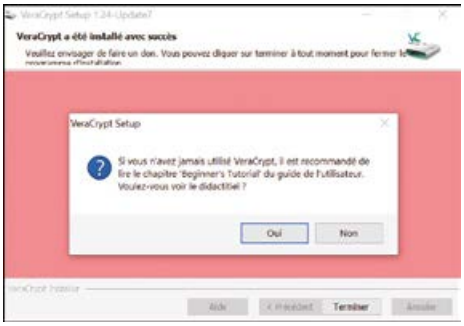
Faites un double clic sur le fichier exécutable. Vous allez peut-être devoir entrer votre mot de passe administrateur ou confirmer votre choix ❶. L'assistant d'installation se lance, choisissez la langue d'installation, puis acceptez les termes du contrat de licence ❷ :



Laissez l'option Installer et cliquez sur le bouton **Suivant** ❸. Vous pouvez laisser le dossier d'installation par défaut, puis cliquez sur le bouton **Installer** ❹ :

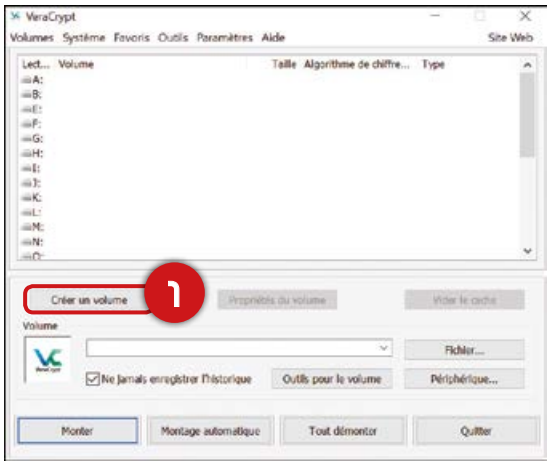


Lorsque l'installation est terminée, vous allez être invité à lire le guide d'utilisation de l'outil :



Créer un fichier conteneur chiffré

Lancez VeraCrypt en double-cliquant sur le raccourci crée sur votre bureau ou dans le menu Démarrer. La fenêtre principale de l'outil s'affiche. Cliquez sur **Créer un volume** ❶ :

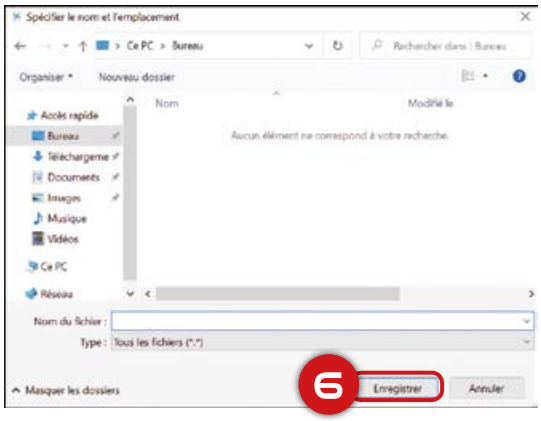


La fenêtre de l'assistant de création de volumes de données devrait apparaître. Laissez la première option qui permet de créer un fichier conteneur chiffré ❷ et cliquez sur **Suivant** ❸ :

Sélectionnez le type de volume, standard ou caché, puis cliquez sur **Suivant** ❹ :

À cette étape, vous devez choisir l'endroit où vous souhaitez que le volume de données soit créé. Pour cela, cliquez sur le bouton **Fichier** ❺ :

Choisissez l'emplacement (par exemple, sur le bureau, dans un dossier particulier ou sur une clé USB), nommez le fichier, et enregistrer votre choix ❻. Enfin, cliquez sur le bouton **Suivant** ❼ :

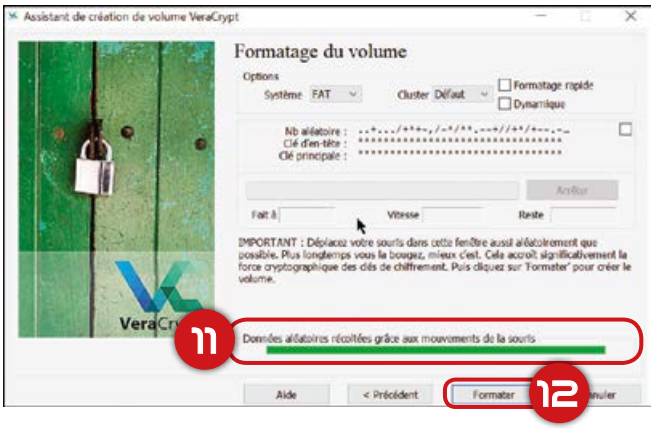


IMPORTANT : Notez que VeraCrypt ne chiffre pas les fichiers existants. Si à cette étape vous choisissez un fichier existant, il sera écrasé et remplacé par le container créé. Vous pourrez chiffrer vos fichiers existants en les déplaçant vers le container VeraCrypt que vous créez maintenant.

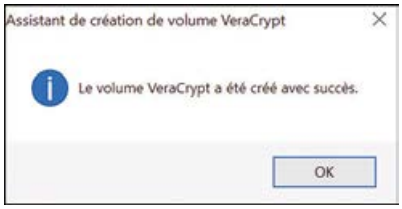
À l'étape suivante, vous avez la possibilité de modifier les options de chiffrements, vous pouvez aussi laisser les valeurs par défaut et cliquer sur **Suivant** ❽ :

Maintenant, définissez la taille du volume ❾, puis un mot de passe robuste qui permettra de le déchiffrer ❿. Sous le champ du mot de passe, vous avez la possibilité d'activer une option de sécurité supplémentaire « Utiliser fichiers clés ». Cette option est facultative et vous permet de ne pouvoir monter le volume (c'est-à-dire, le rendre disponible) qu'en fournissant un certain fichier, appelé un fichier-clé.

À l'étape suivante, déplacez votre souris dans la fenêtre de l'assistant de création de volume aussi aléatoirement que possible et jusqu'à ce que la jauge soit remplie ⓫, puis cliquez sur **Formater** ⓬ :

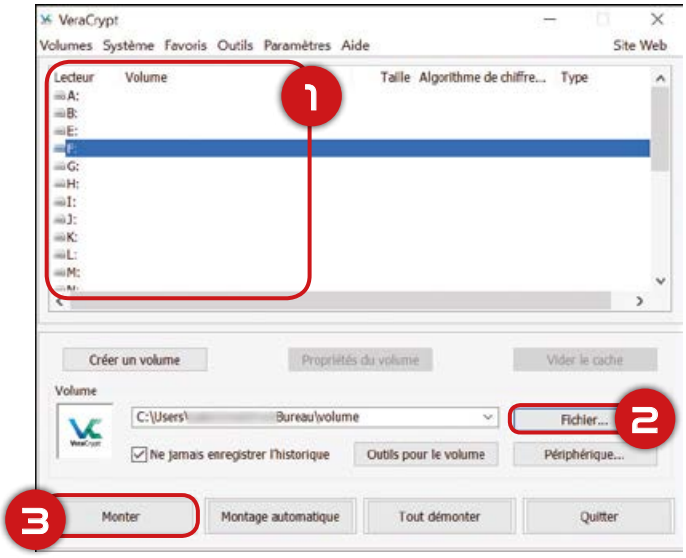


VeraCrypt créé alors un fichier dans l'endroit que vous avez choisi. La création de volume peut prendre un certain temps en fonction de la taille du volume. Quittez l'assistant lorsque vous avez le message assurant la bonne création du volume :

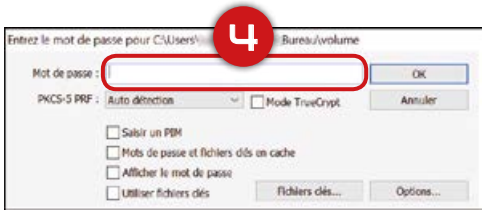


Utiliser le fichier conteneur chiffré

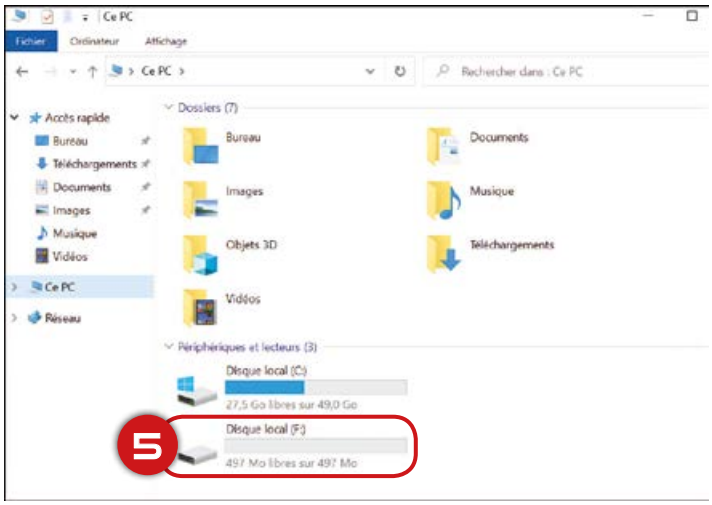
Lancez VeraCrypt, choisissez n'importe quelle lettre de lecteur disponible dans la liste ❶, sélectionnez votre fichier conteneur chiffré ❷ et cliquez sur **Monter** ❸ :



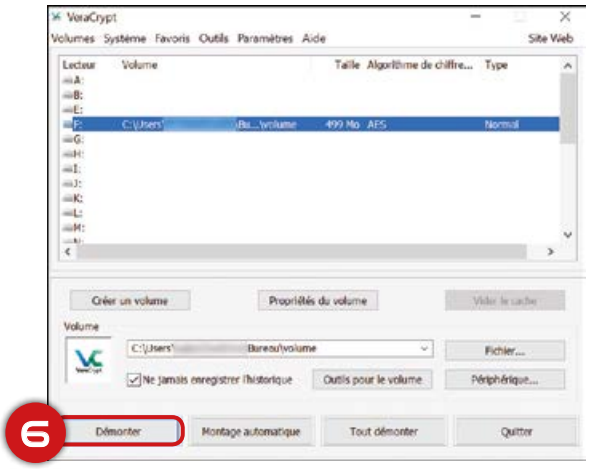
Saisissez le mot de passe du container et cliquez sur **OK** (4) :



Si le mot de passe est correct, le containeur est monté en tant qu'un lecteur local (disque dur) sous la lettre que vous avez choisie 5. Il est visible, par exemple, dans le gestionnaire de fichiers. Vous pouvez l'ouvrir comme un simple disque dur et y déposer des fichiers que vous voulez protéger :



Lorsque vous avez fini de vous servir de votre containeur, n'oubliez pas de le démonter. Pour cela rendez-vous sur l'interface principale de VeraCrypt, sélectionnez votre conteneur dans la liste, puis cliquez sur le bouton **Démonter** 6 **:**

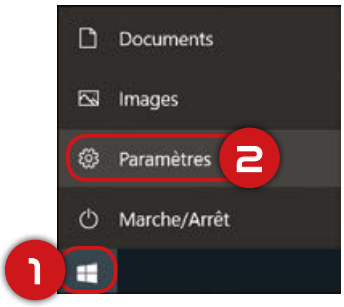


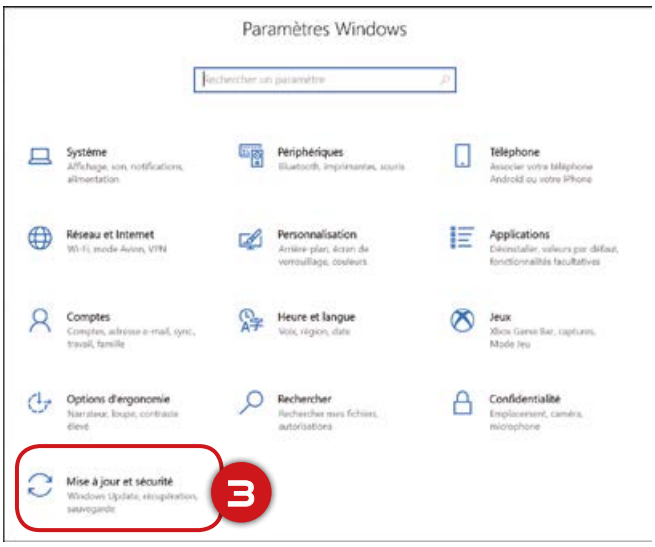
Si vous voulez supprimer le conteneur créé, il suffit de supprimer le fichier correspondant puis de vider la corbeille. Cependant, toutes les données qu'il contenait seront supprimées également.

Sauvegarder les fichiers

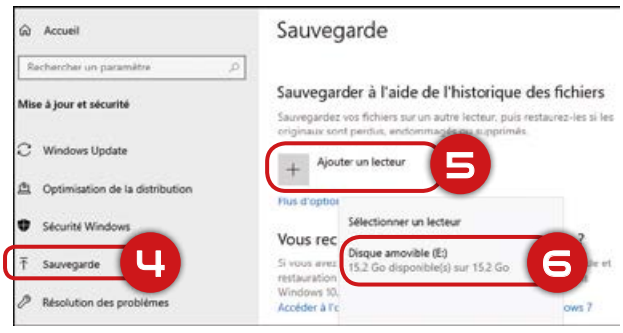
L'outil de Windows **Historique des fichiers** enregistre vos données personnelles sur un disque dur ou une clé USB, vous permettant ainsi de restaurer, par exemple, un fichier supprimé par erreur, ou une version antérieure d'un document modifié. Notez que l'outil **Historique des fichiers** ne sauvegarde pas votre système ni vos programmes, pour cela, reportez-vous au tutoriel «Sauvegarder Windows 10 à l'aide d'une image système».

Tout d'abord, connectez votre lecteur amovible (disque dur ou clé USB) vide et formaté prévu pour la sauvegarde. Ensuite, cliquez sur l'icône **Démarrer** 1, puis **Paramètres** 2. Dans la fenêtre **Paramètres Windows** qui s'affiche choisissez **Mise à jour et sécurité** 3 :



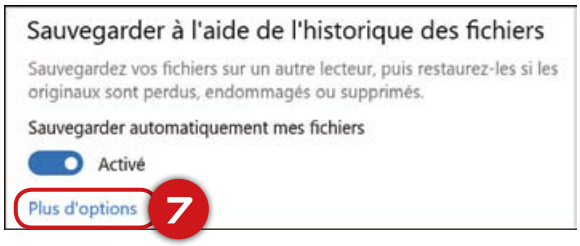


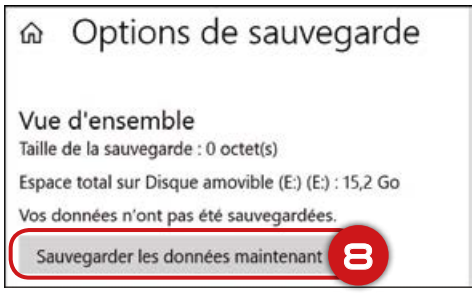
Dans la barre de menu latérale, choisissez **Sauvegarde** 4, puis cliquez sur **Ajouter un lecteur** 5. Sélectionnez votre lecteur prévu pour la sauvegarde 6 dans la liste qui s'affiche :



Si votre lecteur ne s'affiche pas, essayez de l'éjecter, puis rebrancher le à nouveau.

Après avoir sélectionnez votre lecteur, vous allez cliquer sur **Plus d'options** 7.
La fenêtre **Options de sauvegarde** s'affiche alors. Vous pouvez créer votre première sauvegarde en cliquant sur **Sauvegarder les données maintenant** 8 :



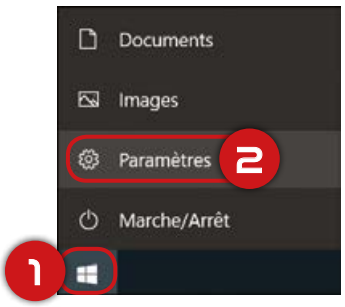


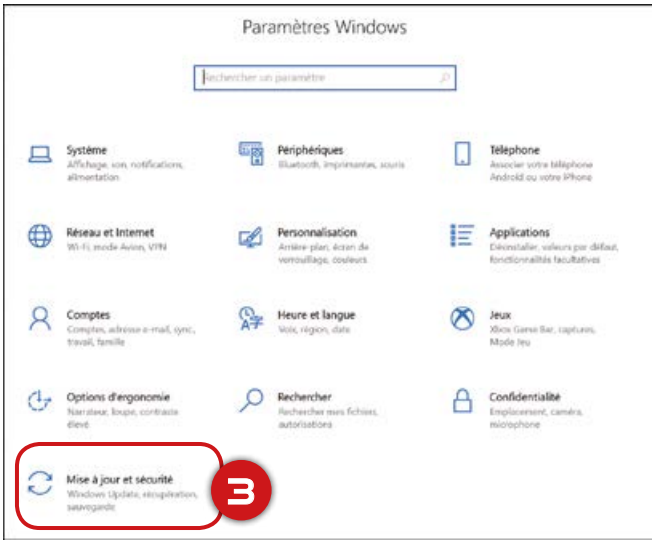
Par défaut, l'outil **Historique des fichiers** sauvegarde les dossiers personnels de votre compte utilisateur (Bureau, Documents, Téléchargements, Musique, Images, Vidéos). Vous pouvez ajouter ou exclure certains dossiers de la sauvegarde.

La durée de la sauvegarde dépend du volume de vos données. Quand la sauvegarde est terminée, n'oubliez pas d'ejecter et déconnecter votre lecteur. Faites les sauvegardes régulières (quotidiennes, hebdomadaires) afin que vos données soient protégées.

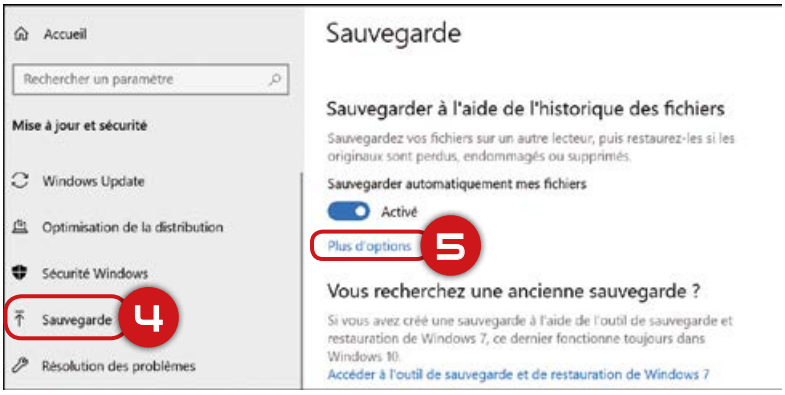
Restaurer les fichiers

Afin de restaurer vos fichiers sauvegardés avec l'outil **Historique des fichiers**, connectez votre disque dur contenant la sauvegarde. Cliquez sur l'icône **Démarrer** ❶, puis **Paramètres** ❷. Dans la fenêtre **Paramètres Windows** qui s'affiche choisissez **Mise à jour et sécurité** ❸ :

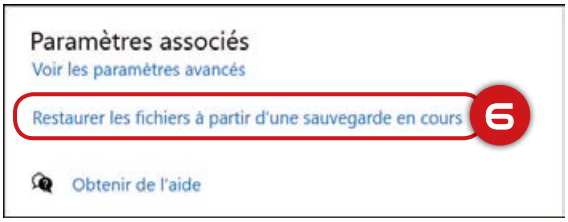




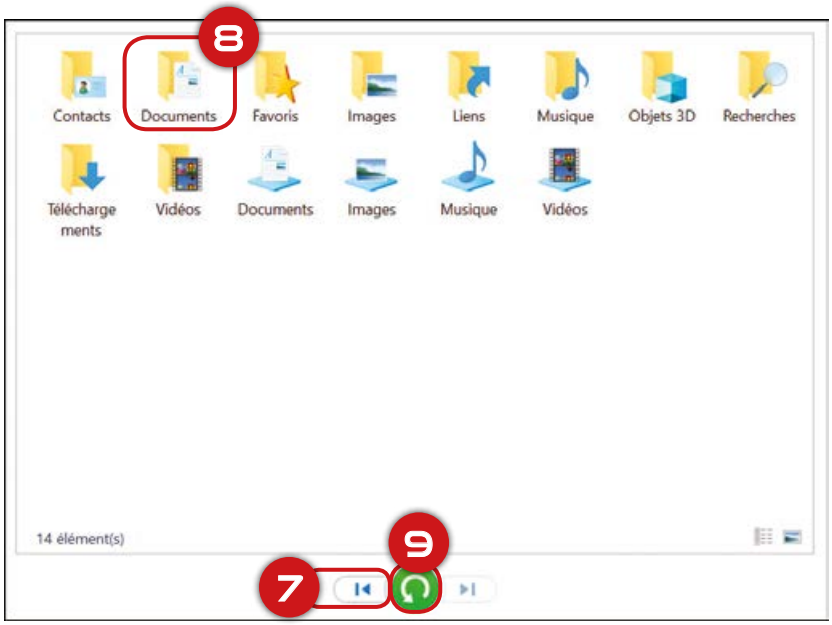
Dans la barre de menu latérale choisissez **Sauvegarde** ❹, puis cliquez sur **Plus d'options** ❺ :



Descendez tout en bas de la fenêtre **Options de sauvegarde** et cliquez sur **Restaurer les fichiers à partir d'une sauvegarde en cours** ❻ :



Cette action permet d'ouvrir l'outil **Historique des fichiers**. Vous pouvez alors naviguer dans les sauvegardes précédentes 7, afin de sélectionner 8 et restaurer vos données **à leur emplacement initial** 9 :



Après avoir restauré vos fichiers, n'oubliez pas d'éjecter et déconnecter votre lecteur amovible.

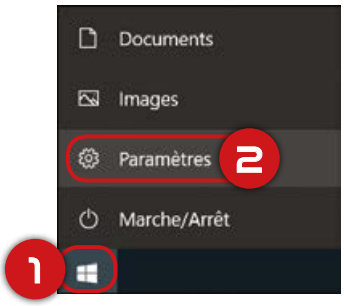
Sauvegarder Windows 10 à l'aide d'une image système

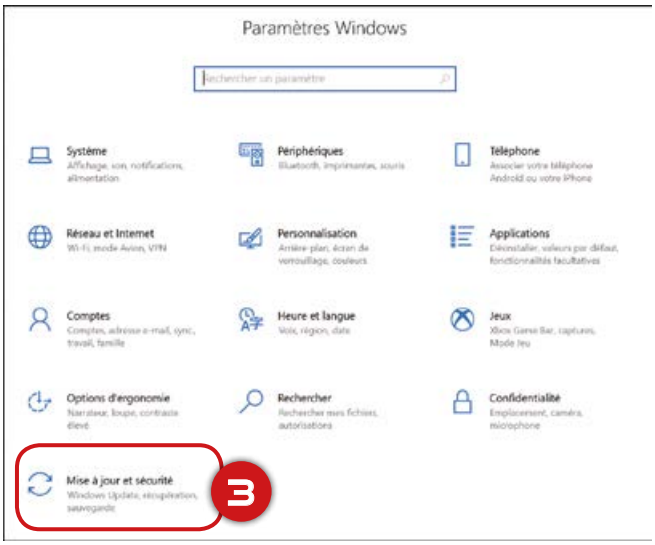
(+ Vidéo)

Windows permet de sauvegarder votre système sur un lecteur amovible (par exemple, un disque dur externe) à l'aide d'une **image système**. Cette méthode de sauvegarde est très pratique pour restaurer un ordinateur après une infection virale ou à la suite de problèmes techniques. Vous devez donc effectuer cette sauvegarde lorsque votre système fonctionne parfaitement.

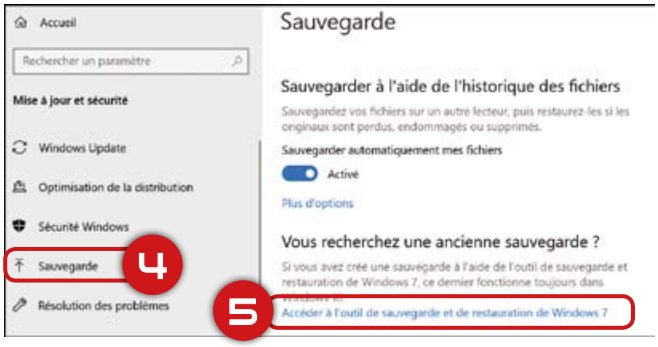
Lorsque vous restaurez votre ordinateur à partir d'une image système (voir le tutoriel « Restaurer Windows 10 à partir d'une image système »), vous retrouvez votre environnement Windows, vos programmes installés, les mises à jour et vos paramètres utilisateurs, ainsi que vos documents/fichiers qui étaient présents dans l'image système. Toutefois, cet outil n'est pas recommandé pour sauvegarder et restaurer vos fichiers, car ceux derniers évoluent très souvent. Pour sauvegarder vos données, nous vous recommandons d'utiliser l'outil de Windows 10, appelé **Historique des fichiers** (voir le tutoriel « Sauvegarder les fichiers »).

Tout d'abord branchez le disque dur externe prévu pour sauvegarder l'image de votre système. Ensuite, cliquez sur **Démarrer** 1, puis **Paramètres** 2. Dans la fenêtre des paramètres Windows, choisissez **Mise à jour et sécurité** 3 :



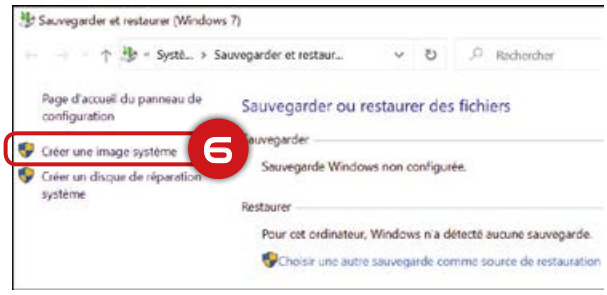


Dans la barre de menu latérale, choisissez **Sauvegarde** 4, puis cliquez sur **Accéder à l'outil de sauvegarde et de restauration de Windows 7**[88] 5 :

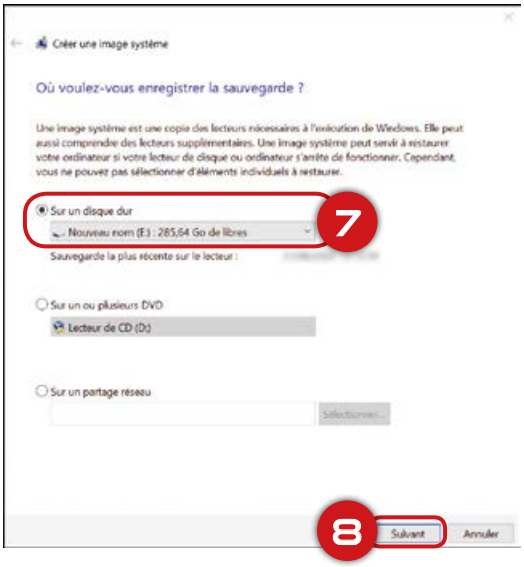


88 Disponible dans Windows 10, cet outil est cependant hérité du système Windows 7.

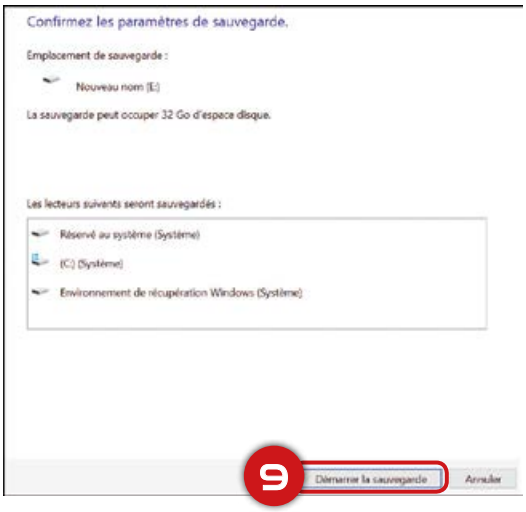
Dans la nouvelle fenêtre qui s'ouvre, cliquez sur **Créer une image système** ❻ :



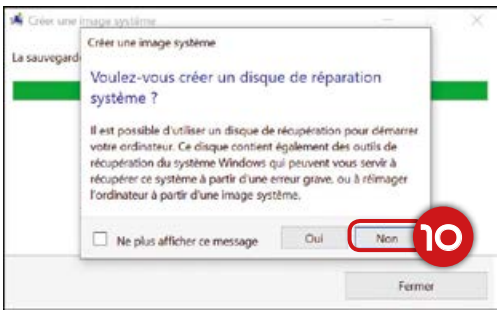
Choisissez la destination de la sauvegarde système, par exemple un disque dur externe ❼ et cliquez sur **Suivant** ❽ :



Sachez que la sauvegarde du système n'est pas possible sur une clé USB.



Confirmez les paramètres de sauvegarde en cliquant sur **Démarrer la sauvegarde** ❾ :



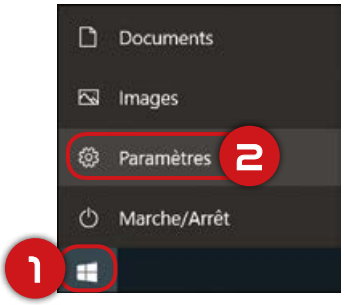
Pendant la sauvegarde, vous allez être invité à créer un **disque de réparation système**. Il s'agit d'un support DVD qui peut vous aider à réparer Windows en cas d'erreur grave. Toutefois, nous vous conseillons de créer la version USB du disque de réparation, appelé **lecteur de récupération du système**[89] (voire le tutoriel « Créer un lecteur de récupération du système »). Refusez donc la création du disque de réparation système ❿, puis, à la fin de sauvegarde éjectez et débranchez votre disque dur.

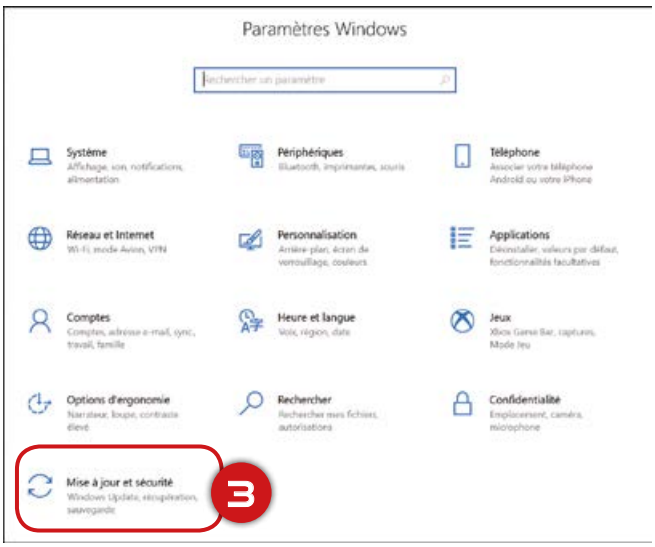
89 Contrairement au disque de réparation système, un **lecteur de récupération inclut les fichiers système Windows qui offrent la possibilité de réinstaller Windows 10 de manière « propre » à partir de votre lecteur.**

Restaurer Windows 10 à partir d'une image système

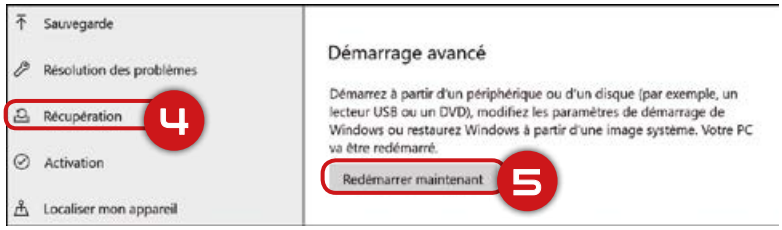
(+ Vidéo)

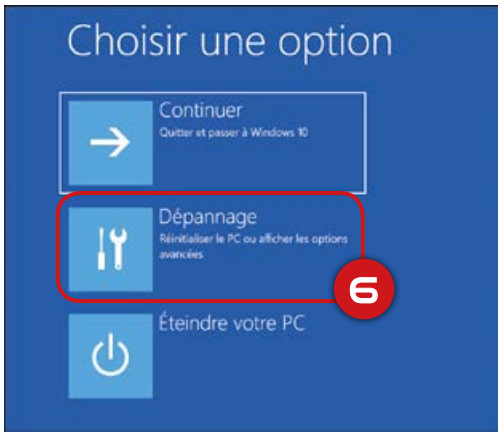
Afin de restaurer le système Windows 10, branchez le disque externe contenant l'image de votre système (voir le tutoriel « Sauvegarder Windows 10 à l'aide d'une image système »), puis accédez aux **Options de démarrage avancées**. Pour cela, cliquez sur **Démarrer** ❶, puis **Paramètres** ❷. Dans la fenêtre des paramètres Windows, choisissez **Mise à jour et sécurité** ❸ :



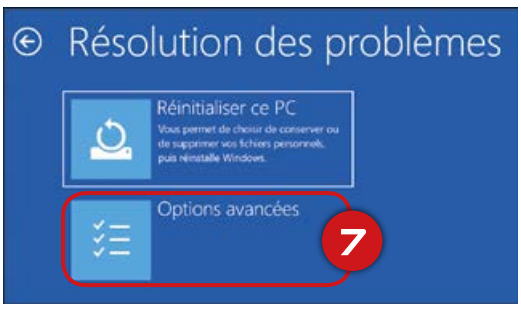


Dans la barre de menu latérale, choisissez **Récupération** ❹, puis dans la zone « Démarrage avancée » cliquez sur **Redémarrer maintenant** ❺ :



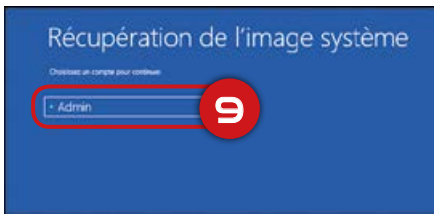


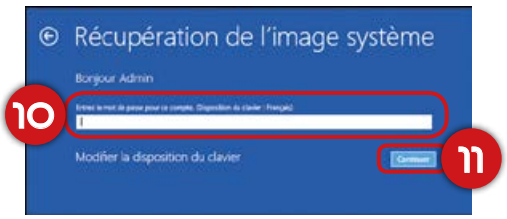
Vous êtes désormais dans les **Options de démarrage avancées** de Windows 10. Choisissez **Dépannage** ❻, puis **Options avancées** ❼ :



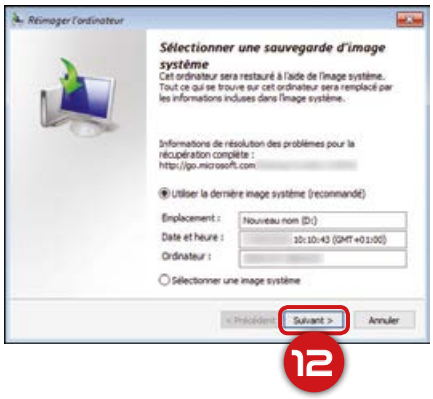
Enfin, choisissez l'option **Récupération de l'image système** 8 :

Votre ordinateur va redémarrer automatiquement. Après redémarrage, connectez-vous avec un compte administrateur 9 10 11 :

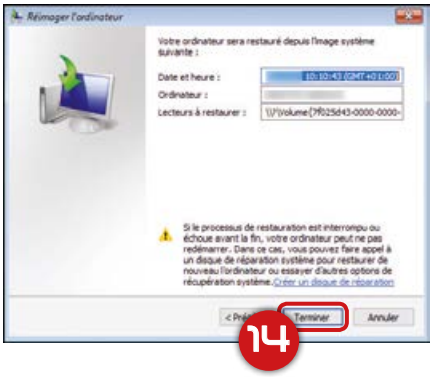


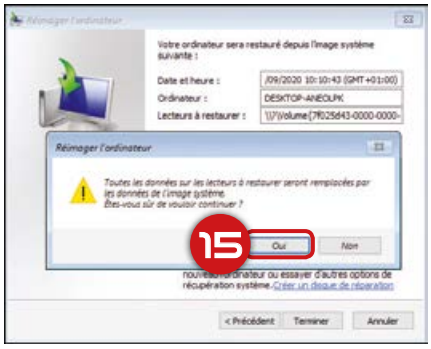


Une boite de dialogue s'ouvre et vous invite à sélectionner la sauvegarde qui vous intéresse. Il est recommandé d'utiliser la dernière image système disponible. Cliquez sur le bouton **Suivant** 12. Choisissez les options de restauration supplémentaires (si c'est possible), puis cliquez sur **Suivant** 13 :

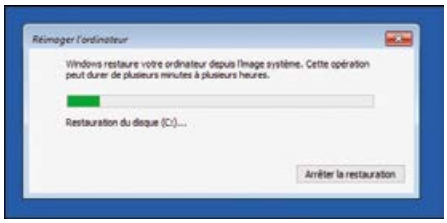


Enfin, cliquez sur le bouton Terminer 14. Le système vous prévient que toutes les données présentes sur vos disques dur internes seront remplacées par les données de l'image système. Confirmez votre choix en cliquant sur le bouton **Oui** 15 :





Le processus de restauration peut durer de plusieurs minutes à plusieurs heures, si vous utilisez un ordinateur portable, pensez donc à le branchez au secteur d'alimentation.

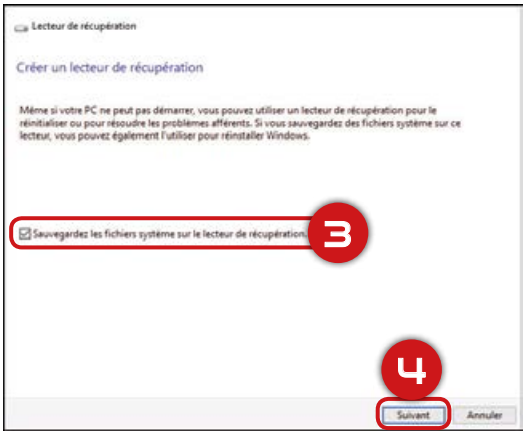


Après la restauration, votre ordinateur va redémarrer et vous allez retrouver votre système Windows, ainsi que tous les logiciels et les fichiers personnels qui étaient présents dans l'image système.

Créer un lecteur de récupération du système

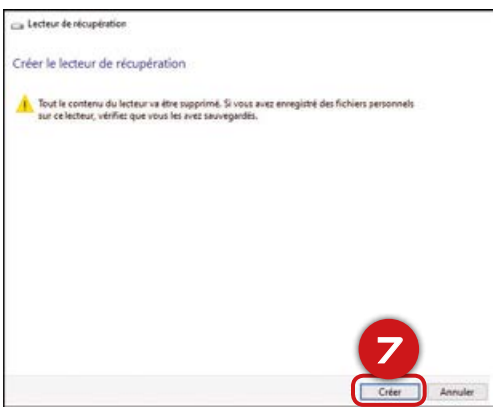
Un lecteur de récupération système est une clé USB **bootable**[90] qui permet de réinstaller votre système lorsque votre ordinateur rencontre un problème majeur. Notez que cet outil ne permet pas de sauvegarder vos fichiers, paramètres ou programmes personnels (voir les tutoriels « Sauvegarder les fichiers » et « Sauvegarder Windows 10 à l'aide d'une image système »).

Dans la zone de recherche[91] sur la barre des tâches, saisissez « lecteur de récupération » ❶, puis choisissez l'application **Lecteur de récupération** ❷. Vous devrez peut-être saisir votre mot de passe administrateur ou confirmer votre choix. A l'ouverture de l'outil, sélectionnez l'option **Sauvegardez les fichiers système sur le lecteur de récupération** ❸, puis cliquez sur **Suivant** ❹ :



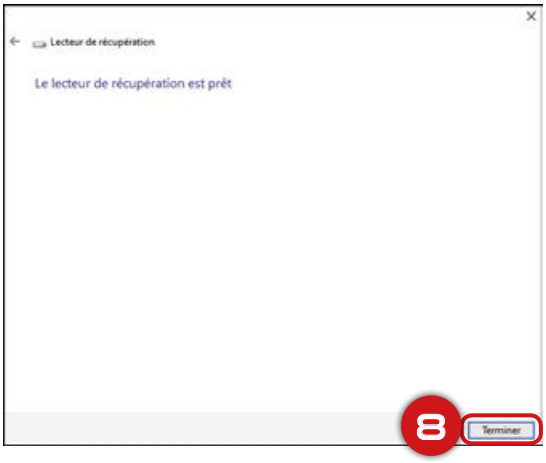
Vous devez patienter plusieurs minutes afin que l'outil prépare les fichiers système, puis, vous allez être invité à connecter une clé USB. En fonction de votre système, la clé doit avoir une capacité égale ou supérieure à 8, 16 ou 32 Go.

Sélectionnez votre clé ❺ et cliquez sur **Suivant** ❻. Un message d'avertissement vous prévient que toutes les données qui sont déjà stockées sur la clé seront effacées. Utilisez donc une clé USB qui ne contient pas de données. Appuyez sur **Créer** ❼ :



90 Il s'agit d'une clé USB à partir de laquelle un ordinateur peut démarrer pour installer ou réparer un système d'exploitation.
91 Si la zone de recherche est invisible, regarder le tutoriel « Afficher les extensions des fichiers ».

De nombreux fichiers vont être copiés sur la clé USB (lecteur de récupération), ce qui peut prendre un certain temps (plusieurs dizaines de minutes à quelques heures). Branchez donc votre ordinateur sur le secteur et ne l'éteignez pas. A la fin du processus, cliquez sur le bouton **Terminer** 8, puis éjectez et déconnectez votre clé USB :



N'utilisez cette clé de récupération qu'en cas d'un problème qui empeche de démarrer Windows normalement.

Crédit photos : ©istock-Rawpixel, MicroStockHub, monkeybusinessimages, solarseven, metamorworks, ipopba, Tinpixels, M_a_y_a, gremlin - ©123RF-dolgachov.
Mise en page : Delphine Le Breton - Impression : MicroLynx

PÔLE D'EXCELLENCE
CYBER

12 B rue du Patis Tatelin
35700 RENNES
France

www.pole-excellence-cyber.org