000-4-Protéger le système – sécurité informatique

➢ Comptes de session Windows : [Support Microsoft]

L'utilisation de comptes protégés par mot de passe pour ouvrir une session Windows est fortement recommandé (mais pas obligatoire) et permet la gestion des personnes auxquelles on souhaite donner la possibilité d'utiliser l'ordinateur.

L'utilisation de comptes permet d'assurer un certain degré d'intégrité, de confidentialité et de sécurité du système Windows lui-même, des logiciels et des applications installées et des données utilisateurs aussi bien dans le cadre d'une utilisation normale de l'ordinateur que pour se prémunir de toutes opérations néfastes, volontaires ou non, dans les cas de perte, vol, prêt ou de partage de la machine.

L'ordinateur doit être configuré avec deux comptes « Administrateur » et au moins un compte utilisateur « Standard ».

. Les mots de passe des comptes « Administrateur » ne doivent être connus que du seul propriétaire et/ou responsable de la machine.
. Les comptes « Administrateur » ne doivent être utilisés que pour des opérations conséquentes, impactant le système, les logiciels et les applications installées (ex : opérations de maintenance, mises à jour, ajouts, modifications, suppressions de fonctionnalités des programmes ou des applications, …)
. En utilisation courante (en mode local ou connecté), utiliser de préférence un compte « Standard », même le propriétaire et/ou responsable de la machine.
. En cas de partage de la machine entre plusieurs personnes, le propriétaire utilisera un des comptes « Administrateur » pour créer autant de comptes « Standard » que nécessaire.

Les mots de passe des comptes Windows doivent être robustes.

. Les mots de passe doivent être construits avec au moins 12 caractères comportant des lettres majuscules, minuscules, chiffres, caractères spéciaux (recommandation CNIL). Ils ne doivent avoir aucun lien de près ou de loin avec des informations personnelles des différents utilisateurs de la machine (des noms, des prénoms, des dates de naissance de personnes ou d'animaux de compagnie, fleurs préférées, …).

Les mots de passe des comptes Windows ne doivent jamais être communiqués.

. Les mots de passe ne doivent jamais et sous aucun prétexte être communiqués à quiconque pour un partage ou un prêt temporaire de la machine, même à une personne connue. Si besoin, le propriétaire de la machine créera un compte « Standard » temporaire supplémentaire.

Les mots de passe des comptes Windows doivent être sauvegardés de manière sécurisée.

. La protection et la sauvegarde des mots de passe sont de la responsabilité du propriétaire et/ou responsable de la machine. Ils ne doivent jamais être conservés en clair mais sauvegardés de manière sécurisée sur au moins deux supports différents et indépendants de la machine (ex : fichier protégé, codé, crypté sur support amovible personnel, sur espace ou cloud opérateur, …).

Les comptes Windows et les mots de passe associés doivent être gérés par le propriétaire et/ou responsable de la machine.

. Les diverses créations, modifications, suppressions des comptes Windows sont de la responsabilité du propriétaire et/ou responsable de la machine.
. En cas de perte ou d'oubli de son mot de passe, l'utilisateur « Standard » doit s'adresser au propriétaire et/ou responsable de la machine. Celui-ci réattribuera un mot de passe temporaire à l'utilisateur qui se chargera ensuite de modifier celui-ci en respectant les règles de configuration des mots de passe.

Configurer l'ouverture de session Windows avec un code PIN (Windows 10).
. Un code confidentiel Hello est plus sécurisé qu'un mot de passe dans le fait que celui-ci est lié physiquement à l'appareil sur lequel il a été configuré.
Le code confidentiel est local à l'appareil, il n'est transmis nulle part et n'est pas stocké sur le serveur

Ne jamais laisser la machine sans surveillance avec une session Windows ouverte.
. En cas d'absence même de très courte durée il est recommandé de verrouiller la session Windows. Utiliser la combinaison de touches Win+L.

Pour créer des comptes Windows par les paramètres de Windows :
Paramètres >> Comptes >> Famille et autres utilisateurs >> Autres utilisateurs …

Pour gérer les comptes Windows par le panneau de configuration :
Panneau de configuration >> Comptes d'utilisateurs >> Comptes d'utilisateurs …

Pour gérer les comptes Windows par le God mode :
Comptes d'utilisateurs >> …

Bonne pratique : Si vous devez envoyer votre ordinateur pour réparation, sauvegardez d'abord tous vos fichiers confidentiels puis supprimez les de l'ordinateur. Supprimez également tous les réglages de mots de passe.

➢ Comptes Microsoft :

Utiliser un compte famille adulte ou enfant pour mieux gérer le prêt ou le partage de la machine.

Il est recommandé d'ajouter et de mettre à jour les informations de sécurité d'un compte Microsoft associé à un compte Windows.
. Les informations de sécurité sont une adresse e-mail ou un numéro de téléphone supplémentaire que l'on peut ajoutez à un compte Windows.
. En cas de saisies multiples et erronées du mot de passe par oubli ou si quelqu'un tente de pirater un compte Windows, Microsoft envoie automatiquement un code de sécurité à l'adresse e-mail ou au numéro de téléphone de secours qui a été associé au compte. Lorsque ce code est renvoyé, Microsoft est alors en mesure d'identifier l'utilisateur et de rétablir l'accès au compte Microsoft.

Utiliser les informations de sécurité d'un compte Microsoft associé à un compte Windows (@mail ou n° tél) pour en vérifier l'activité.
. Se connecter au compte Microsoft concerné puis sélectionner et cliquer sur l'onglet **Sécurité** puis sélectionner et cliquer sur le bouton **Consulter l'activité**.

➢ Créer des points de restauration du système : [Support Microsoft]

Cette opération utilise la protection du système pour annuler toute modification système indésirable. Elle peut aider à corriger des problèmes qui ralentissent l'ordinateur ou l'empêche de répondre. Elle n'affecte pas les données personnelles. Les programmes et les pilotes récemment installés peuvent être désinstallés.

On peut le voir comme un cliché du système d'exploitation à un instant donné. Un point de restauration doit être réalisé avant toute grosse modification importante d'applications ou de logiciels, le système devant être alors dans un état stable.

Cette opération ne prend que quelques minutes, utilise une fonctionnalité de Windows et ne nécessite donc aucune installation logicielle.

Commentaire :
Dans le cas de mise à jour importante de Windows, un point de restauration est automatiquement créé par le système …

Pour accéder à la protection du système :

Saisir **point de restauration** dans la zone de recherche de la barre des tâches >> Fenêtre **Propriétés système**, onglet **Protection du système** >> …

Cliquer sur le bouton **Configurer** puis choisir d'activer ou de désactiver la protection du système et fixer l'espace disque maximal pour cette opération.

Cliquer sur le bouton **Créer** pour créer immédiatement un point de restauration pour les lecteurs dont la protection système est activée …

➢ Créer un lecteur de récupération : [Support Microsoft]

Il est recommandé de créer un lecteur de récupération. Ainsi, si le PC rencontre un problème majeur comme une défaillance matérielle, on utilisera le lecteur de récupération pour le réinitialiser ou pour résoudre les problèmes afférents.

Si les fichiers système ont également été sauvegardés alors le lecteur pourra être aussi utilisé pour réinstaller la version de Windows qui a été utilisé pour le créer. La clé USB ainsi créée n'est pas bootable.

Le lecteur de récupération n'est pas une image système. Il ne contient pas les fichiers, les paramètres ou les programmes personnels.

Il est recommandé de recréer le lecteur chaque année, car les mises à jour Windows améliorent régulièrement la sécurité et les performances du PC.

La création se fera sur un lecteur USB d'au moins 16 gigaoctets vide, car ce processus efface les données qui sont déjà stockées sur le lecteur (les disques ne sont pas une option disponible).

Saisir **Créer un lecteur de récupération** dans la zone de recherche de la barre des tâches >> Suivre les instructions …

Attention : L'opération peut durer plusieurs heures. Il est donc recommandé de la réaliser avec l'ordinateur connecté au secteur et de désactiver la mise en veille et l'arrêt de la machine. Une fois démarrée, l'opération ne doit pas être interrompue !!!

➢ Créer une image système du disque avec WindowsImageBackup : [Support Microsoft]

Une image disque, en tant que fichier compressé, est une copie exacte du disque dur de l'ordinateur, il contient toutes les données du disque dur, y compris le système d'exploitation, les informations de démarrage, les applications et les fichiers individuels. On utilise une image disque dans les cas suivants :

Protection des données : La plupart des utilisateurs créent une image disque pour éviter la perte de données en raison d'un virus, d'une panne système ou d'une défaillance du disque dur. Ainsi, lorsque le disque dur est hors service ou en panne, on achète un nouveau disque dur pour y restaurer l'image disque et remettre l'ordinateur dans un état normal.

Migration de système : L'image disque permet de cloner l'OS d'un disque HDD vers un disque SSD plus performant ou bien de migrer l'OS sur un autre ordinateur qui dispose d'un meilleur matériel.

Déploiement du système d'exploitation : Des grandes entreprises ont souvent besoin d'acheter un grand nombre de nouveaux ordinateurs avec un matériel identique. L'installation du système exploitation et des programmes sur les ordinateurs un par un nécessite beaucoup de temps et d'efforts. Les administrateurs système préfèrent créer une image disque avec un environnement bien préparé afin de rapidement déployer l'OS sur chaque ordinateur. Cette méthode permet d'économiser du temps et des efforts.

L'image doit être réalisée sur un support externe, formaté avec le système de fichiers NTFS, lorsque le système fonctionne parfaitement.

Si le disque à sauvegarder comporte plusieurs partitions, celles-ci peuvent être incluses. Il suffit de les cocher depuis la fenêtre Quels lecteurs souhaitez-vous inclure dans la sauvegarde ?

L'opération dure environ 1 heure.

Par mesure de sécurité, il est souhaitable de créer une sauvegarde à chaque modification importante du système. On peut conserver plusieurs versions d'images sur des disques durs internes ou externes. Les images système plus anciennes sont supprimées lorsque le lecteur est saturé. Le support n'est pas dédié, la sauvegarde se trouve dans le dossier WindowsimageBackup et on peut continuer à l'utiliser pour d'autres usages.

Créer une image système Windows par le panneau de configuration :
Panneau de configuration >> **Système et sécurité** >> **Sauvegarder et restaurer (Windows 7)** >> **Créer une image système …**
Créer une image système Windows par le God mode :
Sauvegarder et restaurer (Windows 7) >> …

➢ Sécurité informatique en mode local :

Ne jamais utiliser de machine avec un OS et/ou des logiciels obsolètes (liste sur CERT-FR). L'état du système et de ses protections doivent être régulièrement mis à jour et fréquemment vérifiés.
. Des mises à jour sont fréquemment envoyées automatiquement sur la machine. Il est impératif de ne pas gêner, d'empêcher ou de bloquer l'installation de ces mises à jour (soit manuellement soit en installant des programmes qui gênent et bloquent l'installation de ces mises à jour).

Effectuer régulièrement des sauvegardes du système.
. Il est recommandé de vérifier régulièrement et manuellement (au moins une fois par mois) l'état des mises à jour du BIOS, du système, de l'antivirus, du pare-feu et de faire des sauvegardes (points de restauration).

Vérifier et contrôler les installations de logiciels depuis des supports mobiles.
Eviter d'installer des logiciels depuis des unités de stockage externe de source non fiable (clé USB, disque externe, DVD, …). Préférer les installations en réseau depuis les sites officiels des éditeurs des logiciels ou le Windows store …

Pour limiter voire interdire l'installation de logiciels indésirables et/ou non vérifiés, il est recommandé de désactiver l'exécution automatique des programmes depuis des supports mobiles (autorun) voire même de désactiver les ports de connexion des dispositifs externes et interdire leur utilisation.
. Eviter d'installer des logiciels gratuits de sources inconnues, préférer des logiciels payants préconisés et recommandés par Microsoft (sur son magasin Microsoft Windows), par le SILL ou d'éditeurs et de sources connues et certifiées.
. Utiliser un antivirus pour analyser un programme douteux avant de l'utiliser

Si plusieurs personnes utilisent la machine désactiver les ports USB. Ceux-ci ne seront ouverts que sur demande à un administrateur qui s'assurera du bienfondé de l'opération à l'origine de la demande …
Gestionnaire de périphériques >> Développer **Contrôleurs de bus USB** >> **Périphérique USB composite** >> **Pilote** >> **Désactiver l'appareil …**
Faire l'opération inverse pour les réactiver …

Fixer le critère sur l'origine des applications à installer.
Paramètres >> **Applications** >> **Applications et fonctionnalités** >> **Choisir l'origine des applications …**

Vérifier et contrôler avant utilisation les fichiers avec des extensions .com, .exe, .bat et les macros des logiciels comme word ou excel, powerpoint, …).

Ne jamais utiliser des données personnelles sur une machine inconnue même prêtée par une personne de confiance.

➢ Sécurité informatique en mode connecté :

Avant la navigation :

Ne jamais utiliser de machine avec un OS, un navigateur et/ou des logiciels obsolètes (liste sur CERT-FR). L'état du système Windows et de ses protections, le navigateur, l'antivirus, le pare-feu utilisé, le contrôle parental éventuellement, doivent être régulièrement mis à jour et fréquemment vérifiés.

Ne jamais utiliser un ordinateur inconnu, même prêté par une connaissance.

Ne jamais utiliser des points d'accès WIFI publics pour se connecter à des sites qui demandent la saisie de données personnelles et privées.

Naviguer de préférence avec une session Windows « Standard » et pas « Administrateur ». Créer et configurer si besoin un compte temporaire lors d'un prêt de l'ordinateur.

Hors connexion réseau (ignorer la notification qui s'affiche), ouvrir le menu du navigateur pour procéder au paramétrage de la sécurité en local (Paramétrage >> Options >> Vie privée et sécurité >> …)

- **Interdire l'enregistrement des identifiants et des mots de passe pour les sites web ...**
- **Effacer et Interdire la conservation de l'historique et du suivi de navigation (cookies) ...**
- **Activer la protection contre le pistage ...**
- **Activer la protection contre les contenus trompeurs et les logiciels dangereux ...**

Enregistrer les modifications apportées, fermer le navigateur et rétablir la connexion réseau.

Pendant la navigation :

Naviguer sur le Web que sur des sites vérifiés, sécurisés et certifiés …
Utiliser de préférence la navigation privée pour naviguer …
Utiliser des connexions sécurisées et cryptées de bout en bout (https://)
Ne se connecter qu'à des sites sécurisés, authentifiés et certifiés …
Utiliser le clavier virtuel pour saisir des données confidentielles (logiciels espions qui interceptent les saisies du clavier physique de l'ordinateur)
Vérifier les adresses de destination des liens hypertextes depuis les pages visitées (passer sur le lien avec la souris pour l'afficher), en cas de doute et si nécessaire taper manuellement l'adresse souhaitée directement dans le champ de recherche du navigateur …

A la fin de la navigation :

Veiller à bien fermer les sessions ouvertes avec les sites visités et à bien se déconnecter (logout) …
Avant de quitter le navigateur, veiller à bien fermer tous les onglets ouverts …
S'assurer et vérifier éventuellement le bon effacement de l'historique de navigation.

Sauvegarder ses données : **[Support Microsoft] ; [Support Microsoft]**

Les données doivent être sauvegardées fréquemment, manuellement ou automatiquement à l'aide d'un logiciel de sauvegarde, sur au moins un support externe (clé USB, CD, disque externe, NAS, cloud …) pour se prémunir de toute perte ou altération suite à une attaque virale ou à une panne logicielle ou matérielle.

Solution Windows 10 pour réaliser des sauvegardes :
Paramètres >> **Mise à jour et sécurité** >> **Sauvegarde** …

Règle absolue : Le support de sauvegarde ne doit jamais voyager en compagnie de l'ordinateur.

➢ Sources et références :

Commission Nationale Informatique et Liberté [CNIL]
Agence Nationale de Sécurité des Système d'Information [ANSSI]
Socle Interministériel des Logiciels Libres (SILL), [Wikipedia],[SILL]
Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques [CERT-FR]
Confédération des PME [CPME]