ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Protéger les données et le poste informatique

www.ofppt.info

Sommaire

1. Introduction

Après l'installation du système d'exploitation et des applications utilisateur, les utilisateurs seront amené à travailler sur différentes données « fichiers, dossiers et logiciels » et aussi utiliser la messagerie électronique et par conséquent ils utiliseront la connexion internet.

Si vous êtes connecté à Internet, que vous autorisez d'autres personnes à utiliser votre ordinateur ou que vous partagez des fichiers avec d'autres utilisateurs, vous devez prendre certaines mesures afin de protéger l'ordinateur de tout dommage éventuel. Pourquoi ? Parce qu'il existe des escrocs informatiques (parfois appelés *utilisateurs malveillants* ou *pirates informatiques*) qui attaquent les ordinateurs d'utilisateurs tiers. Ces individus peuvent attaquer directement, en accédant à votre ordinateur via Internet et en s'appropriant vos informations personnelles, ou indirectement en créant un logiciel malveillant (ou *programme malveillant*) conçu pour endommager votre ordinateur.
Heureusement, vous pouvez vous protéger en prenant quelques précautions simples. Cet article décrit les menaces éventuelles et les actions à prendre pour s'en protéger.

2. Sauvegarde de fichiers et de dossiers

L'utilitaire de sauvegarde (ex : NTBACKUP) vous permet de sauvegarder des données dans un fichier ou sur une bande. Lorsque vous sauvegardez des données dans un fichier, vous devez spécifier le nom et l'emplacement du fichier à enregistrer. Les fichiers de sauvegarde portent généralement l'extension .bkf, mais vous pouvez la remplacer par n'importe quelle extension de votre choix. Un fichier de sauvegarde peut être enregistré sur un disque dur, une disquette ou tout autre **support amovible ou fixe** permettant l'enregistrement d'un fichier.

Lorsque vous sauvegardez des données sur une bande, un périphérique à bande doit être connecté à votre ordinateur. Les bandes sont gérées par le **Stockage amovible**. Bien que l'utilitaire de sauvegarde fonctionne avec le Stockage amovible, ce dernier peut vous servir à effectuer certaines tâches de maintenance telles que la préparation et l'éjection de bandes.
Les quatre étapes suivantes décrivent une opération de sauvegarde simplifiée :

2.1. Sélectionner des fichiers, des dossiers et des lecteurs en vue d'une sauvegarde

L'utilitaire de sauvegarde (ex : NTBACKUP) affiche une arborescence des lecteurs, fichiers et dossiers de votre ordinateur qui peut vous servir à sélectionner les fichiers et les dossiers à sauvegarder. Cette arborescence s'utilise de la même façon que l'Explorateur Windows pour ouvrir des

lecteurs ou des dossiers et sélectionner des fichiers.

2.2. Sélectionner le média de stockage ou l'emplacement des fichiers des données sauvegardées

L'utilitaire de sauvegarde offre deux options pour la sélection du média de stockage :
Vous pouvez sauvegarder vos données **dans un fichier sur un périphérique de stockage**. Un périphérique de stockage peut être un disque dur, une disquette Zip ou tout type de média amovible ou fixe permettant l'enregistrement d'un fichier. Cette option est toujours disponible.
Vous pouvez sauvegarder vos données sur un périphérique à bande. Cette option n'est disponible que si un périphérique à bande est installé sur votre ordinateur ou connecté à ce dernier. Si vous sauvegardez des données sur un périphérique à bande, le média est géré par le Stockage amovible.

2.3. Définir les options de sauvegarde

La boîte de dialogue **Options** est à votre disposition pour personnaliser vos opérations de sauvegarde. La boîte de dialogue **Options** vous permet d'effectuer les actions suivantes :

Sélectionner le type de sauvegarde à effectuer. Les options possibles sont : **copie, quotidienne, différentielle, incrémentielle et normale**.

Choisir d'enregistrer vos actions de sauvegarde dans un fichier journal. Si vous activez cette option, vous avez également la possibilité de choisir un fichier journal complet ou un fichier journal résumé.

Choisir de sauvegarder les données stockées sur des lecteurs montés.

Spécifier les types de fichiers à exclure d'une opération de sauvegarde.

Choisir de vérifier si les données ont été correctement sauvegardées.

2.4. Démarrer la sauvegarde

Lorsque vous démarrez une opération de sauvegarde, vous êtes invité à entrer des informations sur cette tâche, tout en ayant la possibilité de configurer des options avancées. Une fois que vous avez fourni les informations ou modifié les options nécessaires, la sauvegarde des fichiers et des dossiers sélectionnés démarre.
Si vous planifiez une exécution sans assistance, vous devez néanmoins fournir des informations sur l'opération de sauvegarde à effectuer. Cependant, une fois ces informations fournies, la sauvegarde des fichiers ne démarre pas avant d'avoir été ajoutée au Planificateur de tâches.

Remarques

- Vous devez être un administrateur ou un opérateur de sauvegarde pour pouvoir sauvegarder des fichiers et des dossiers. Si vous êtes membre du groupe Utilisateurs ou Utilisateurs avec pouvoir, vous devez être propriétaire des fichiers et dossiers que vous voulez sauvegarder ou disposer d'une ou plusieurs des autorisations suivantes pour les fichiers et les dossiers à sauvegarder : Lecture,

Lecture et exécution, Modification ou Contrôle total.

- Le Registre, le service d'annuaire et d'autres composants système clés sont contenus dans les données sur l'état du système. Pour sauvegarder ces composants, vous devez sauvegarder les données sur l'état du système.
- Vous ne pouvez sauvegarder les données sur l'état du système que sur un ordinateur local. Vous ne pouvez pas sauvegarder les données sur l'état du système sur un ordinateur distant.
- Vous pouvez planifier une sauvegarde pour qu'elle s'exécute sans assistance, à une heure ou selon une fréquence spécifique. Vous pouvez planifier une sauvegarde après avoir cliqué sur Démarrer.
- Si les services Windows Media sont actifs sur votre ordinateur et que vous souhaitez sauvegarder les fichiers associés à ces services, consultez « Exécuter une sauvegarde avec les services Windows Media » dans la documentation en ligne des services Windows Media. Vous devez suivre les procédures décrites dans la documentation en ligne des services Windows Media avant de sauvegarder ou de restaurer les fichiers associés aux services Windows Media.
- Si vous utilisez le Stockage amovible pour gérer des médias, ou le Stockage étendu pour stocker des données, vous devez sauvegarder régulièrement les fichiers situés dans les dossiers suivants :

Systemroot\System32\Ntmsdata
Systemroot\System32\Remotestorage
Cela permet de garantir la restauration de la totalité des données du Stockage étendu et du Stockage amovible.

2.5. Utilisation de l'utilitaire de sauvegarde

Pour ouvrir Utilitaire de sauvegarde

- Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Accessoires**, sur **Outils système**, puis cliquez sur **Utilitaire de sauvegarde**.
- Le service de stockage amovible doit être démarré pour que l'utilitaire de sauvegarde fonctionne correctement
- Sinon, vous pouvez utiliser l'Assistant Récupération automatique du système de l'utilitaire de sauvegarde pour vous aider à réparer votre système.
- Pour plus d'informations sur l'emploi de l'utilitaire de sauvegarde, cliquez sur le menu **?** (Aide) de cet utilitaire

2.5.1. Utilisation du Stockage amovible

Vous devrez peut-être ouvrir une session en tant qu"administrateur ou en tant que membre du groupe Administrateurs pour effectuer certaines tâches.

Le composant Stockage amovible vous permet de gérer facilement les supports de stockage amovibles (bandes et disques optiques, par exemple), ainsi que les bibliothèques qui les contiennent (telles que les changeurs et les juke-boxes).

Pour ouvrir le Stockage amovible

1. Cliquez sur **Démarrer**,
2. Puis sur **Panneau de configuration**.
3. Double-cliquez sur **Outils d"administration**
4. Puis sur **Gestion de l"ordinateur**
5. Dans l'arborescence de la console, cliquez sur **Stockage amovible**.

2.5.2. Configurer le Stockage amovible

Étape	Référence
Vérifiez que vous disposez d'une bibliothèque prise en charge.	Pour trouver le matériel pris en charge par les systèmes d"exploitation Windows, visitez le Catalogue Windows sur le site Web de Microsoft.
Installez et testez la bibliothèque.	Consultez le guide d'utilisation de la bibliothèque et suivez les recommandations du fabricant. Prêtez particulièrement attention à la numérotation des emplacements et des types de média pris en charge, et vérifiez si les lecteurs nécessitent un nettoyage périodique.
Créez des pools de médias prenant en charge les applications, selon vos besoins.	Pour créer un pool de médias.
Déplacez suffisamment de médias vers un pool de médias libre.	Pour déplacer un média ou un disque vers un autre pool de médias.
Définissez des autorisations utilisateur ou de groupe pour le Stockage amovible, selon vos besoins.	Pour modifier les autorisations d'utilisateur pour le Stockage amovible.

2.6. Pour créer un point de restauration

1. Accédez à l'Assistant Restauration du système via le Centre d'aide et de support.
2. Cliquez sur **Créer un point de restauration**, puis sur **Suivant**.
3. Dans la zone **Description du point de restauration**, tapez un nom identifiant ce point de restauration. La Restauration du système ajoute automatiquement à ce nom la date et l'heure de création du point de restauration.
   - Pour terminer la création du point de restauration, cliquez sur **Créer**.
   - Pour annuler la création du point de restauration et revenir à l'écran **Restauration du système**, cliquez sur **Précédent**.

- Pour annuler la création du point de restauration et quitter l'Assistant Restauration du système, cliquez sur **Annuler**.

Remarques

- Pour accéder à l"Assistant Restauration du système, cliquez sur **Démarrer**, puis sur **Aide et support**. Cliquez sur **Performances et maintenance**, sur **Utilisation de Restauration du système pour annuler des modifications**, puis sur **Exécuter l"Assistant Restauration du système**.
- Vous pouvez avoir intérêt à créer un point de restauration lorsque vous prévoyez d'apporter au système des modifications risquées ou susceptibles de rendre l'ordinateur instable.
- Pour afficher ce point de restauration ou y revenir, dans l'écran **Restauration du système** de l'Assistant Restauration du système, sélectionnez **Restaurer mon ordinateur à une heure antérieure**. Ensuite, sélectionnez la date de création du point de restauration à partir du calendrier de l'écran **Sélectionnez un point de restauration**. Tous les points de restauration créés à la date sélectionnée sont répertoriés par leur nom dans la zone de liste située à droite du calendrier.

3. Alimentation de secours

L'onduleur est un Périphérique connecté entre un ordinateur et une source d'alimentation pour garantir une alimentation électrique ininterrompue. Les onduleurs utilisent des batteries pour permettre le fonctionnement d'un ordinateur pendant une courte période de temps après une panne de courant. Les onduleurs fournissent également une protection contre les pointes et les baisses de tension.

3.1. Utilisation du service de l'onduleur

Après avoir fait l'acquisition d'un **Uninterruptible Power Supply (UPS)** pour votre ordinateur, vous pouvez utiliser le **service de l'onduleur** pour définir ses options de fonctionnement à l'aide des Options d'alimentation dans le Panneau de configuration. L'onglet **Onduleur** dans les Options d'alimentation vous permet de contrôler le mode de fonctionnement du service de l'onduleur sur votre ordinateur. Les paramètres d'onduleur disponibles dépendent de l'onduleur spécifique installé sur votre système. Les paramètres peuvent inclure des options telles que :

- Le port série auquel est connecté l'onduleur.
- Les circonstances qui déclenchent l'envoi d'un signal par l'onduleur, telles qu'une panne de courant d'un utilitaire, un faible niveau de batterie et l'arrêt à distance par l'onduleur.
- Les intervalles de temps consacrés à l'entretien des batteries, au rechargement de la batterie et à l'envoi de messages d'avertissement après une panne de courant.

3.2. Pour configurer un onduleur

Vous devez avoir ouvert une session en tant qu"administrateur ou en tant que membre du groupe Administrateurs pour pouvoir effectuer cette procédure. Si votre ordinateur est connecté à un réseau, les paramètres de stratégie réseau peuvent également vous empêcher d"effectuer cette procédure.

1. Dans le Panneau de configuration, ouvrez les **Options d'alimentation**.
2. Sous l'onglet **Onduleur**, cliquez sur **Configurer**.
3. Dans la boîte de dialogue **Configuration de l'onduleur**, modifiez un ou plusieurs des paramètres suivants :

3.2.1. Activer toutes les notifications

- Activez cette case à cocher si vous souhaitez que le Uninterruptible Power Supply (UPS) service Windows affiche un message d'avertissement lorsque l'ordinateur bascule sur l'alimentation de l'onduleur. Vous pouvez indiquer le délai d'attente en secondes avant l'affichage du message initial d'avertissement de panne de courant et le nombre de secondes qui doivent s'écouler avant d'afficher les messages de panne de courant suivants.

3.2.2. Alarme critique

- Activez la case à cocher **Temps restant en minutes de fonctionnement sur batteries avant l'alarme critique** si vous souhaitez que Windows permette à l'ordinateur de fonctionner sur UPS pendant un nombre de minutes défini avant d'effectuer l'alarme d'alimentation critique.
- Activez la case à cocher **Lorsque l'alerte se produit, exécuter ce programme** si vous voulez que Windows exécute un programme ou une tâche lorsque l'onduleur déclenche l'alerte d'alimentation critique.
    1. Cliquez sur **Configurer**.
    2. Dans la boîte de dialogue **Extinction de l'onduleur**, dans **Exécuter**, tapez le programme ou la tâche à exécuter avant que l'onduleur n'arrête l'ordinateur, ou cliquez sur **Parcourir** pour rechercher un programme ou une tâche.
    3. Sous l'onglet **Planification**, personnalisez la planification de la tâche comme il convient.
    4. Sous l'onglet **Paramètres**, personnalisez les paramètres appropriés pour l'exécution de la tâche planifiée, le temps d'inactivité et la gestion de l'alimentation.
- Dans la liste **Ensuite, demandez à l'ordinateur de**, cliquez sur l'état du système dans lequel vous souhaitez que l'ordinateur entre lors de l'alarme d'alimentation critique.
- Activez la case à cocher **Finalement, mettre l'onduleur hors tension** si vous souhaitez que l'onduleur s'arrête en même temps que l'ordinateur.

4. Protection contre les virus et les chevaux de Troie

Dans le monde informatique moderne, vous devez protéger votre ordinateur et votre réseau contre les intrusions intentionnelles, qui se matérialisent sous la forme de virus et de chevaux de Troie. Suivez ces conseils pour éviter la propagation de virus et les attaques de chevaux de Troie.

Pour les utilisateurs :

- Documentez-vous sur les virus et la façon dont ils se répandent généralement. Vous pouvez involontairement infecter le réseau en chargeant un programme à partir d'une source comme Internet, un forum électronique en ligne ou des pièces jointes à des messages électroniques.
- Familiarisez-vous avez les symptômes les plus courants des virus : messages inhabituels apparaissant à l'écran, baisse des performances du système, données manquantes et incapacité à accéder à votre disque dur. Si vous remarquez l'un de ces problèmes sur votre ordinateur, lancez immédiatement votre logiciel de détection de virus pour réduire les risques de perte de données.
- Les programmes sur disquettes peuvent également contenir des virus. Analysez toutes les disquettes avant de copier ou d'ouvrir des fichiers à partir de celles-ci, ou de les utiliser pour démarrer votre ordinateur.
- Ayez au minimum un programme de détection de virus et utilisez-le régulièrement pour vérifier que vos ordinateurs ne sont pas infectés. Assurez-vous que vous disposez bien des derniers fichiers de signature de virus pour votre programme lorsque ceux-ci sont disponibles, car de nouveaux virus sont créés chaque jour.

Pour les administrateurs :

- Avant de placer un nouveau programme sur le réseau, installez celui-ci sur un ordinateur non connecté au réseau et procédez à une vérification à l'aide de votre logiciel de détection de virus. (Même s'il est conseillé de vous connecter à votre ordinateur en tant que membre du groupe Utilisateurs, vous devez installer le programme lorsque vous êtes connecté en tant que membre du groupe local Administrateurs car tous les programmes ne sont pas installés avec succès lorsque cette opération est effectuée par un membre du groupe Utilisateurs.)
- Ne laissez pas les utilisateurs se connecter en tant que membres du groupe Administrateurs sur leur propre ordinateur car les virus peuvent faire plus de dégâts s'ils sont activés à partir d'un compte possédant des autorisations d'administration. Les utilisateurs doivent se connecter en tant que membres du groupe Utilisateurs afin de ne posséder que les autorisations nécessaires pour exécuter leurs tâches.
- Demandez aux utilisateurs de créer des mots de passe forts pour que les virus ne puissent pas trouver facilement les mots de passe et obtenir des autorisations d'administration. (Vous pouvez définir les exigences en matière de mot de passe à l'aide du composant enfichable Stratégie de

groupe.) Pour obtenir des informations sur la création de mots de passe forts, cliquez sur **Rubriques connexes**.

- Sauvegardez régulièrement les fichiers afin de réduire les dommages causés par un virus.
- Quelques antivirus gratuits :

  Avast : http://www.avast.com/eng/download-avast-home.html
  AVG : http://free.grisoft.com/freeweb.ph [...] /us/tpl/v5
  Antivir : http://www.free-av.com/

Remarque

Pour plus d'informations sur les virus, consultez la documentation de votre logiciel de détection de virus.

5. Centre de sécurité Windows:

Le Centre de sécurité Windows représente le quartier général de la sécurité de votre ordinateur. Il affiche le statut de sécurité actuel de votre ordinateur et effectue des recommandations sur les actions qui doivent être prises pour améliorer sa sécurité. Pour l'ouvrir :

Pour ouvrir le Centre de sécurité, cliquez sur le bouton **Démarrer**, sur **Panneau de configuration**, sur **Sécurité**, puis sur **Centre de sécurité**.

Le Centre de sécurité vérifie la présence sur l'ordinateur des éléments suivants indispensables à sa sécurité :

- **Pare-feu.** Un pare-feu peut protéger l'ordinateur en empêchant les pirates informatiques et les logiciels malveillants d'y accéder.
- **Mises à jour automatiques**. Windows peut rechercher régulièrement la présence des mises à jour pour l'ordinateur, et les installer automatiquement.
- **Protection contre les programmes malveillants**. Un logiciel antivirus peut protéger l'ordinateur contre les virus, les vers et autres atteintes à la sécurité. Un logiciel anti-espion peut protéger l'ordinateur contre les logiciels espions et les logiciels potentiellement nuisibles
- Autres paramètres de sécurité. Le Centre de sécurité vérifie que les paramètres de sécurité Internet sont appropriés et détermine si le contrôle du compte utilisateur est activé.

5.1. Utiliser un pare-feu

Un pare-feu est un logiciel ou un matériel qui vérifie les informations provenant d'Internet ou d'un réseau, puis les empêche d'accéder à l'ordinateur ou les y autorise, selon vos paramètres de pare-feu définis. Il contribue ainsi à empêcher que des pirates informatiques ou des logiciels malveillants n'accèdent à l'ordinateur.
Le Pare-feu Windows, intégré à Windows, est activé automatiquement.
Si vous exécutez un programme, par exemple un programme de messagerie instantanée ou un jeu en réseau multijoueur qui doit recevoir des informations provenant d'Internet ou d'un réseau, le pare-feu vous demande si vous souhaitez bloquer ou débloquer (autoriser) la connexion. Si vous décidez de débloquer la connexion, le pare-feu Windows crée une exception pour ne pas vous déranger lorsque ce programme aura besoin de recevoir des informations à l'avenir.

L'onglet Général du Pare-feu Windows comporte trois paramètres. Voici ce que vous pouvez faire avec ces paramètres et quand les utiliser :

5.1.1. Activé (recommandé)

Ce paramètre est sélectionné par défaut. Lorsque le Pare-feu Windows est activé, la communication à travers le feu est bloquée pour la plupart des programmes. Si vous souhaitez débloquer un programme, vous pouvez l'ajouter à la liste des exceptions (dans l'onglet Exceptions). Par exemple, vous ne pourrez peut-être pas envoyer des photos à l'aide d'un programme de messagerie instantanée avant d'avoir ajouté ce programme à la liste des exceptions.

5.1.2. Bloquer toutes les connexions

Ce paramètre bloque toutes les tentatives non sollicitées de connexion à votre ordinateur. Utilisez ce paramètre lorsque vous avez besoin d'une protection maximale pour votre ordinateur, par exemple lorsque vous vous connectez à un réseau public dans un hôtel ou un aéroport ou lorsqu'un ver dangereux se répand sur Internet. Si ce paramètre est activé, vous n'êtes pas averti lorsque le Pare-feu Windows bloque tous les programmes, et les programmes de la liste des exceptions sont ignorés.
Lorsque vous sélectionnez Bloquer toutes les connexions, vous pouvez quand même afficher la plupart des pages Web, et recevoir et envoyer du courrier électronique ainsi que des messages instantanés.

5.1.3. Désactivé (non recommandé)

Évitez d'utiliser ce paramètre à moins qu'un autre pare-feu ne soit exécuté sur votre ordinateur. La désactivation du Pare-feu Windows peut rendre votre ordinateur (et votre réseau si vous en utilisez un) plus vulnérable à des attaques de pirates informatiques ou de logiciels malveillants tels que des vers.

Remarque

1. Si certains paramètres du pare-feu ne sont pas disponibles et que votre ordinateur est connecté à un domaine, votre administrateur système contrôle probablement ces

paramètres via une stratégie de groupe.

Si l'un des éléments de la sécurité apparaît sur un arrière-plan rouge ou jaune, cela signifie que l'ordinateur peut être vulnérable aux atteintes à la sécurité. Pour résoudre le problème, cliquez sur un élément pour le développer, puis suivez les instructions.

5.2. Que sont les alertes de sécurité ?

Si Windows détecte que l'ordinateur requiert une configuration de sécurité renforcée dans l'un des domaines de sécurité (pare-feu, mise à jour automatique, protection contre les programmes malveillants ou autres paramètres de sécurité), il affiche une notification à chaque ouverture de session, jusqu'à ce que le problème soit résolu. Les notifications s'affichent dans la zone de notification de la barre des tâches.

Cliquez sur la notification pour ouvrir le Centre de sécurité, où vous pouvez apprendre comment régler le problème.

Remarque
Pour désactiver les notifications de sécurité ou masquer l'icône du Centre de sécurité dans la zone de notification, ouvrez le Centre de sécurité, cliquez sur **Modifier la manière dont le Centre de sécurité m'avertit**, puis choisissez une option. Même si vous désactivez les notifications, le Centre de sécurité continuera ses vérifications et affichera l'état de la sécurité.

5.3. Utiliser la protection antivirus

Les virus, les vers et les chevaux de Troie sont des programmes créés par des pirates informatiques qui utilisent Internet pour infecter des ordinateurs vulnérables. Les virus et les vers peuvent se répliquer d'un ordinateur à l'autre, tandis que les chevaux de Troie accèdent à un ordinateur en se cachant à l'intérieur d'un programme apparemment inoffensif, un écran de veille, par exemple. Certains virus, vers et chevaux de Troie nuisibles peuvent supprimer des informations du disque dur ou désactiver totalement l'ordinateur. D'autres ne causent pas de dommages directs, mais dégradent les performances et la stabilité de l'ordinateur.

Les programmes antivirus analysent le courrier électronique et d'autres fichiers de l'ordinateur à la recherche de virus, vers et chevaux de Troie. En cas de détection d'un programme nuisible, l'antivirus met le virus *en quarantaine* (l'isole) ou le supprime complètement, avant qu'il n'endommage l'ordinateur et les fichiers.

Aucun programme antivirus n'est intégré à Windows, mais le fabricant de l'ordinateur peut en avoir installé un. Cliquez sur Centre de sécurité pour vérifier si votre ordinateur est doté d'une protection antivirus. Si ce n'est pas le cas, accédez à la page Web des partenaires antivirus Microsoft pour rechercher un programme antivirus.

Étant donné que de nouveaux virus sont identifiés tous les jours, il est important de choisir un programme antivirus doté d'une fonctionnalité de

mise à jour automatique. Lors de la mise à jour de votre logiciel antivirus, les nouveaux virus sont ajoutés à sa liste de virus à rechercher, ce qui vous protège contre les nouvelles attaques. Si la liste de virus est obsolète, votre ordinateur est vulnérable aux nouvelles menaces. Les mises à jour requièrent généralement le paiement d'un abonnement annuel. Conservez votre abonnement à jour pour recevoir des mises à jour régulières.

Si vous n'utilisez pas de logiciel antivirus, vous exposez l'ordinateur aux menaces de logiciels malveillants. Vous risquez également de transmettre des virus à d'autres ordinateurs.

5.4. Utiliser la protection contre les logiciels espions

Un logiciel espion peut afficher des publicités, collecter des informations vous concernant ou modifier les paramètres de votre ordinateur, généralement sans votre consentement explicite. Par exemple, il peut installer des barres d'outils, des liens ou des favoris non désirés dans votre navigateur Web, modifier votre page d'accueil par défaut ou afficher fréquemment des fenêtres publicitaires intempestives. Avec certains logiciels espions, aucun symptôme ne permet de détecter leur présence, ce qui ne les empêche pas de collecter en secret des informations sensibles, tels que les sites Web que vous visitez ou le texte que vous tapez. La plupart des logiciels espions sont installés en même temps que les logiciels gratuits que vous téléchargez, mais dans certains cas, une simple visite sur un site Web peut entraîner une infection par un logiciel espion.

Pour protéger l'ordinateur contre les logiciels espions, utilisez un programme anti-espion. Cette version de Windows comporte un programme anti-espion intégré appelé Windows Defender, qui est activé par défaut. Windows Defender vous avertit lorsque des logiciels espions tentent de s'installer sur l'ordinateur. Il peut également analyser l'ordinateur à la recherche de logiciels espions et les supprimer.

Étant donné que de nouveaux logiciels espions apparaissent chaque jour, Windows Defender doit être régulièrement mis à jour pour détecter et combattre les menaces de logiciels espions les plus récentes. Windows Defender est mis à jour le ca échéant à chaque mise à jour de Windows. Pour un niveau de protection optimale, définissez Windows afin qu'il installe automatiquement les mises à jour (voir ci-dessous).

5.5. Mettre à jour Windows automatiquement

Microsoft propose régulièrement des mises à jour importantes de Windows qui peuvent permettre de protéger l'ordinateur contre des nouveaux virus et autres atteintes à la sécurité. Pour être sûr de recevoir ces mises à jour le plus rapidement possible, activez la mise à jour automatique. Ainsi, vous n'avez pas à vous inquiéter de savoir si des correctifs critiques pour Windows sont manquants sur l'ordinateur.

Les mises à jour sont téléchargées en tâche de fond lorsque vous êtes connecté à Internet. Elles sont installées à 3 h 00 du matin, sauf si vous spécifiez une heure différente. Si vous éteignez l'ordinateur avant cette

heure, vous pouvez installer les mises à jour avant de l'arrêter. Sinon, Windows les installera au prochain démarrage de l'ordinateur.

5.6. Pour activer la mise à jour automatique

Pour ouvrir Windows Update, cliquez sur le bouton **Démarrer**, sur **Tous les programmes**, puis sur **Windows Update**.

Cliquez sur **Modifier les paramètres.**

Assurez-vous que l'option **Installer les mises à jour automatiquement (recommandé)** est sélectionnée.

Windows installera les mises à jour importantes pour votre ordinateur au fur et à mesure de leur disponibilité.

Les mises à jour importantes fournissent des avantages significatifs, tels qu'une sécurité et une fiabilité améliorées.

Sous **Mises à jour recommandées**, vérifiez que la case à cocher **Inclure les mises à jour recommandées lors du téléchargement, de l'installation ou de la notification de mises à jour** est activée, puis cliquez sur OK.

Les mises à jour recommandées concernent des problèmes non critiques et vous permettent une meilleure utilisation de l'ordinateur.

Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, fournissez le mot de passe ou la confirmation.

6. Utiliser un compte d'utilisateur standard

Lorsque vous ouvrez une session sur l'ordinateur, Windows vous octroie un certain niveau de droits et de privilèges en fonction du type de compte d'utilisateur que vous possédez. Il existe trois différents types de comptes d'utilisateur : standard, administrateur et invité.

Bien qu'un compte d'administrateur fournisse un contrôle total de l'ordinateur, l'utilisation d'un compte standard peut contribuer à le sécuriser. Ainsi, si d'autres utilisateurs (ou pirates informatiques) parviennent à accéder à l'ordinateur lorsque vous êtes connecté, ils ne pourront ni changer ses paramètres de sécurité ni modifier d'autres comptes d'utilisateur.

6.1. Pour déterminer votre type de compte

Pour ouvrir Comptes d'utilisateurs, cliquez sur le bouton **Démarrer**, sur **Panneau de configuration**, sur **Comptes d'utilisateurs et sécurité de la famille** (ou sur **Comptes d'utilisateurs**, si vous êtes connecté à un domaine de réseau), puis sur **Comptes d'utilisateurs**.

Le compte d'utilisateur apparaît sous votre nom.

Si vous utilisez actuellement un compte d'administrateur, voir Modifier le type de compte d'un utilisateur pour savoir comment le transformer en compte standard.

6.2. Conseils pour utiliser le courrier électronique et le Web en toute sécurité

Soyez vigilant lorsque vous ouvrez des pièces jointes. Les pièces jointes (fichiers attachés à des messages électroniques) sont en effet une source principale d'infection par virus. N'ouvrez jamais une pièce jointe qui vous a été envoyée par un inconnu. Si vous connaissez l'expéditeur mais que vous ne vous attendiez pas à recevoir une pièce jointe, vérifiez auprès de celui-ci qu'il vous a effectivement envoyé la pièce jointe avant de l'ouvrir. Voir Quand faire confiance à un message électronique et Éviter les virus transmis par courriers électroniques

Protégez vos informations personnelles. Si un site Web vous demande votre numéro de carte bancaire, vos informations bancaires ou toute autre information personnelle, assurez-vous qu'il s'agit d'un site de confiance et vérifiez que son système de transaction est sécurisé. Voir Quand faire confiance à un site Web.

Utilisez le filtre d'hameçonnage dans Internet Explorer. L'hameçonnage est une pratique consistant à créer des messages électroniques et des sites Web frauduleux afin d'amener par la ruse les utilisateurs à révéler des informations personnelles ou financières. Le message électronique ou le site Web frauduleux semble provenir d'une source de confiance, telle qu'une banque, une société de cartes de crédit ou un commerçant en ligne de confiance. Le filtre d'hameçonnage contribue à détecter les sites Web d'hameçonnage afin de vous protéger des éventuelles escroqueries.

Soyez prudent lorsque vous cliquez sur des liens hypertexte dans des messages électroniques. Les liens hypertexte (liens qui ouvrent des sites Web lorsque vous cliquez dessus) sont souvent utilisés dans le cadre d'escroqueries par hameçonnage ou par logiciel espion, mais ils peuvent également transmettre des virus. Cliquez uniquement sur ces liens s'ils se trouvent dans des messages électroniques de confiance.

Installez des composants additionnels uniquement à partir de sites Web de confiance. Les composants additionnels de navigateur Web, notamment les contrôles ActiveX, permettent aux pages Web d'afficher des éléments tels que des barres d'outils, des téléscripteurs pour le marché boursier, des vidéos et des animations. Cependant, ces composants peuvent également installer des logiciels espions ou d'autres logiciels malveillants. Si un site Web vous demande d'installer un composant additionnel, assurez-vous qu'il s'agit d'un site de confiance avant de poursuivre.

Pour approfondir le sujet....

REPORTER VOUS A LA DOCUMENTATION DE SUPPORT TECHNIQUE MICROSOT WINDOWS XP OU WINDOWS VISTA

Sources de référence

SITE OFFICIELLE MICROSOFT /WINDOWS XP ET WINDOWS VISTA