Configuration de Trend Micro Internet Security (PC-cillin version 11)

Le présent document est une description des opérations de configuration, avec présentation des copies d'écran qui vous apparaîtront « étape par étape ». Les utilisateurs avertis se satisferont du manuel livré avec le logiciel.

Pour les néophytes, cela permet de s'assurer qu'aucune étape n'a été omise. La présentation des copies d'écran, dans l'ordre, permet de se situer à chaque instant dans le déroulement de la configuration.

Le choix du déroulement des opérations est subjectif ; c'est comme cela qu'il nous semble bon de faire pour une première prise en main. Libre à vous de le faire dans un autre ordre, y compris celui proposé par l'écran d'accueil de Trend Micro Internet Security

Tout d'abord :

Télécharger (si ce n'est déjà fait) le fichier à l'adresse suivante : http://diff.ac-creteil.fr/di/Trend/sources/PCC/pccis_win_11_1295_fr.zip

ou

Insérer le cédérom qui vous aura été fourni par une structure d'assistance (PMC, PAI, Personne ressource en Informatique) et installez le logiciel.

Aidez vous si nécessaire des documentations en ligne, pas à pas avec copie d'écran, ou simplifiée pour utilisateur avertis.

Une fois le produit installé, enregistré, mis à jour, vous pouvez mettre en place des protections complémentaires ou affiner la configuration de votre antivirus :

1. activation d'un pare-feu (firewall) protégeant votre ordinateur des attaques venant du réseau ou de l'Internet (bouton Pare-feu)
2. activation du filtrage « anti-spam » (anti pourriel) ; les messages indésirables qui encombrent les boîtes (bouton Courrier électronique)
3. vérification du courrier entrant ET sortant (bouton Courrier électronique)
4. paramétrage fin des fonctions de l'antivirus (bouton Système)
5. Gestion des fichiers mis en quarantaine (bouton Système)
6. Configuration de tâches régulières de scan (bouton Système)
7. configuration de la mise à jour (bouton Mise à jour)
8. activation du filtrage d'URL (d'adresses de sites Internet) (bouton Internet)
9. activation de la protection des données personnelles (bouton Internet)
10. activation d'un mot de passe pour la configuration des deux dernières fonctions (bouton Internet)
11. vérifier votre protection (bouton État)

Accéder aux fonctions de configuration *(c'est la marche à suivre à chaque fois que vous voudrez modifier ou affiner la configuration)*

En bas et à droite de votre écran, parmi les icones situés à gauche de l'horloge se trouve celui de PC-cillin (Trend Micro Internet Security). (reconnaissable à son éclair rouge)

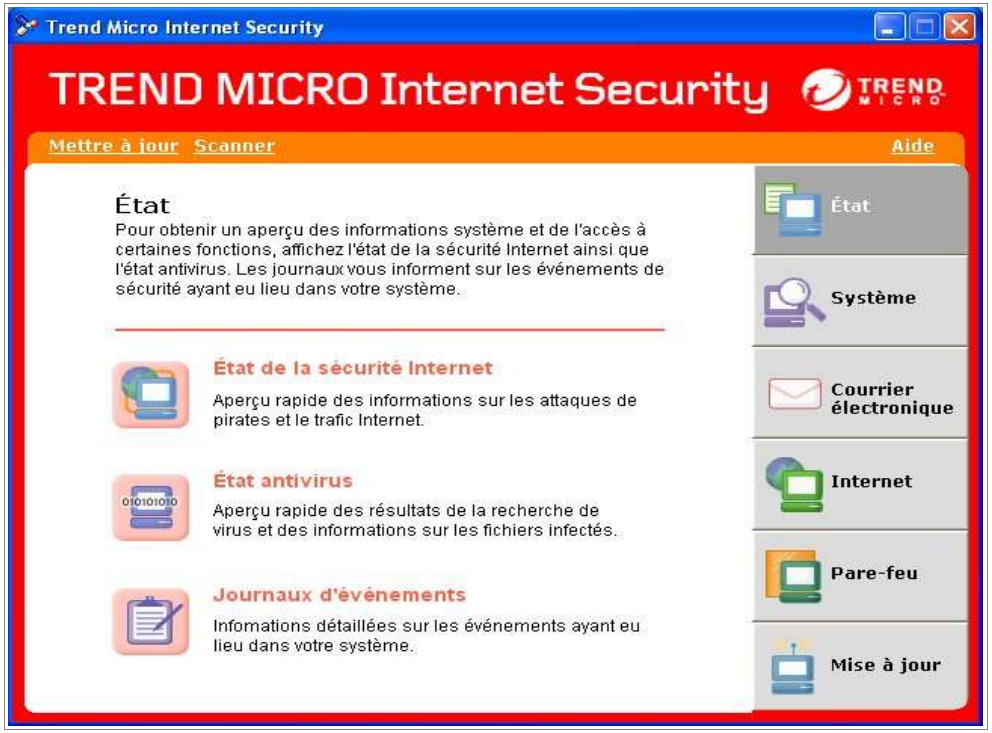
En déplaçant la souris vous obtenez les versions de votre antivirus, moteur et signatures.

(en avril 2004 nous en sommes déjà aux versions 7.100 et 1.855.00)

En cliquant avec le bouton **droit** de la souris sur l'icone <Trend Micro Internet Security> situé en bas et à droite de votre écran, vous ouvrez un menu déroulant, permettant d'accéder à la configuration du logiciel antivirus et la mise à jour immédiate de celui-ci. (cf plus loin page 11)

Le menu ouvert, Cliquer avec le bouton gauche sur « Ouvrir l'écran principal »

Il est possible d'accéder au même écran par <Démarrer/ Programmes/Trend Micro Internet Security/Trend Micro Internet Security>



C'est à partir de cet écran qu'il sera possible de configurer votre antivirus, et c'est par lui que vous passerez pour chaque modification

1. Activation du pare-feu *(pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)*

Cliquer dans la case « Pare-feu » de l'écran d'accueil Trend Micro Internet Security

Cliquer sur le pavé « Profils de pare-feu », une boîte de dialogue s'ouvre.

Cocher la case « Activer le pare-feu personnel » et choisir le profil (image suivante)

Si vous êtes connecté directement via ADSL, choisir connexion directe. Pour ceux qui ont plusieurs machines en réseau, le paramétrage est plus complexe, il est nécessaire de bien lire la documentation Trend et/ou de faire appel à un expert réseau.

Règle générale, cliquer sur « Appliquer » pour que les paramètres puissent être pris en compte, avant chaque changement de menu ou d'écran.
Sinon, vous obtiendrez le message d'erreur suivant.

2. Activation du filtrage « anti-spam » (anti-pourriel) ; *les messages indésirables qui encombrent les boîtes*.

(pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)

Cette fonction rajoute dans l'en-tête « Objet » de votre logiciel de courrier (Thunderbird, Mozilla, Pegasus, Eudora, Netscape, Incredimail, Outlook etc.) le mot « Spam ». Il est alors facile de mettre en place des filtres envoyant ces pourriels, soit dans un dossier prévu à cet effet (conseillé), soit directement à la poubelle.
Attention, *des messages intéressants peuvent avoir être considérés comme du spam, que l'on voudra récupérer, et qu'il est donc judicieux de classer là où l'on pourra les reprendre*.

Cliquer dans la case « Courrier électronique » de l'écran d'accueil Trend Micro Internet Security

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>Cliquer sur le pavé « Anti-spam » une boîte de dialogue s'ouvre.

Cocher la case « Activer la protection anti-spam » et choisir la protection la plus élevée (image suivante)</td>
<td>Il sera toujours possible d'ajouter dans la « liste blanche » les adresses considérées par erreur comme étant du spam (par exemple les annonces de promotions que vous auriez sollicitées du type FNAC, CAMIF etc.)</td>
</tr>
</table>

Il est possible d'éditer la liste blanche, en ajoutant, modifiant, ou supprimant les adresses dont vous acceptez les messages.

Pour modifier ou supprimer, cliquer sur l'adresse pour la mettre en « surbrillance » bleue.

Entrer l'adresse considérée comme « spam » (pourriel), elle ne sera plus étiquetée comme étant du « spam ».

3. Vérification du courrier entrant ET sortant *(pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)*

Cliquer dans la case « Courrier électronique » de l'écran d'accueil Trend Micro Internet Security :
puis Cliquer sur le pavé « Scan du courrier électronique ». Une boîte de dialogue s'ouvre sous cette appellation.

Cocher la case « Activer le scan du courrier entrant (messagerie POP3 ». Les paramètres par défaut conviennent à l'utilisateur normal.

Si votre ordinateur est récent et si vous êtes soit craintif, soit très exposé, voir « parano », augmenter le nombre de couche et la taille des fichiers compressés.

Choisir l'option supprimer pour les fichiers non nettoyables (si ce n'est pas une malversation, votre correspondant vous renverra le fichier « propre »)

Cliquer sur « Appliquer » pour prendre en compte les paramètres pour le courrier entrant puis sur l'onglet « Courrier sortant » en blanc (voir image précédente).

Pour le courrier sortant pratiquer de même que pour le courrier entrant.

<u>Sauf pour les fichiers non nettoyables.</u>

Choisir de les bloquer. Ceci ne devrait cependant pas arriver dans la mesure où votre station est à jour d'antivirus et « scannée » régulièrement.

Comme toujours, cliquer sur « Appliquer » pour que les paramètres puissent être pris en compte.

4. Paramétrage fin des fonctions de l'antivirus *(pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)*

Cliquer dans la case « Système » (colonne de droite) de l'écran d'accueil Trend Micro Internet Security.
Il s'agira, dans l'ordre, de déterminer les paramètres d'analyse (scan), d'analyser les disques afin de vérifier qu'il n'y a aucune trace de virus, de programmer des tâches régulières d'analyse (scan), d'accéder, plus tard, à la liste des fichiers mis en quarantaine (si vous avez choisi cette option).

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>Cliquer sur le pavé « Paramètres ». Une boîte de dialogue s'ouvre où le mot « scan » peut se traduire par « analyse des fichiers et programmes situés sur le(s) disque(s) dur(s) de votre ordinateur».
Vous pouvez configurer les paramètres du scan manuel, que vous déclenchez vous même, et du scan en temps réel qui se lance de façon automatique à l'allumage de la machine. En premier (onglet orange), le scan manuel
Selon le degré de sécurité voulu, fonction de votre utilisation, de la puissance de votre machine ou de votre degré de vulnérabilité, plusieurs options sont offertes.</td>
<td>« Recommandé » est le paramètre de base pour le scan manuel, mais les paramètres suivants sont de bonnes précautions avec une machine récente.
« Tous les fichiers »
« Scanner les fichiers compressés » couches=6
« Inclure les secteur d'amorçage »
« Rechercher et supprimer les chevaux de Troie »
« Action spécifique Nettoyer et Supprimer »
« Supprimer les virus dans les fichiers ZIP »</td>
</tr>
</table>

Cliquez sur l'onglet « Scan en temps réel », il devient orange
« Recommandé » est le paramètre de base pour le Scan en temps réel mais là aussi,les paramètres suivants sont de bonnes précautions avec une machine récente.
« Tous les fichiers »
« Scanner les fichiers compressés » couches=6
« Inclure les secteur d'amorçage »
« Rechercher et supprimer les chevaux de Troie »
« Action spécifique Nettoyer et Supprimer »
« Supprimer les virus dans les fichiers ZIP »

Une fois ceci paramétré, il est judicieux d'analyser votre ordinateur une première fois afin de s'assurer qu'il est exempt de virus.
Cette action devra être renouvelée régulièrement, soit de façon manuelle (colonne suivante) soit de façon automatisée (voir plus loin).

Analyse et Vérification des disques

Cliquer sur la case « Système » puis l'option « Scan des fichiers »

Vous pouvez alors décider de faire analyser (scanner) « Tout », y compris les cédéroms et les disques réseaux....ou,

Choisir le(s) lecteur(s) à analyser. *(Nous conseillons cette usage comme préférable)*

Une fois le choix fait, lancer l'analyse (scan) en cliquant sur le pavé « Scanner », et attendre que s'opère l'analyse jusqu'à son terme.

5. Gestion des fichiers mis en « quarantaine » *(pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)*

Cliquer dans la case « Système » de l'écran d'accueil Trend Micro Internet Security

Cliquer sur le pavé « Quarantaine » une boîte de dialogue s'ouvre.

Si vous avez choisi l'option mise en quarantaine, ces fichiers sont conservés dans un répertoire.

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>Il est possible par ce menu de les nettoyer, supprimer un fichier, de supprimer tous les fichiers ou de restaurer les fichiers sélectionnés.</td>
<td>Un guide de la quarantaine peut s'afficher à chaque consultation (cocher la case) ou en cliquant sur le pavé grisé « Guide de quarantaine »</td>
</tr>
</table>

6. Configuration de tâches régulières de scan *(pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)*

Cliquer dans la case « Système » de l'écran d'accueil Trend Micro Internet Security

Cliquer sur le pavé « Tâches de Scan » une boîte de dialogue s'ouvre. (voire première image du paragraphe 4)

Le mot « scan » et à traduire par « analyse des fichiers et programmes situés sur le disque dur de votre ordinateur».

Vous pouvez choisir et configurer des tâches de scan automatiques.

Celles-ci pourront être journalières, hebdomadaires, mensuelles.

Il est possible d'ajouter, de supprimer, de modifier des tâches.

Pour les modifier ou les supprimer, il faut auparavant les sélectionner (surbrillance bleue)

Le premier onglet « Cible du scan » permet de donner un nom et de choisir les lecteurs à analyser.

Le deuxième onglet « Option de Scan » est similaire aux options vues plus haut

« Recommandé » est le paramètre de base mais,

« Tous les fichiers »
« Scanner les fichiers compressés » couches=6
« Inclure les secteur d'amorçage »
« Rechercher et supprimer les chevaux de Troie »
« Action spécifique Netoyer et Supprimer »
« Désinfecter les fichiers compressés »
sont de bonnes précautions avec une machine récente.

Le troisième onglet permet la programmation véritable :

la fréquence peut être quotidienne, hebdomadaire, mensuelle ou « aucune » pour désactiver une tâche programmée sans perdre les autres réglages.

pour la fréquence mensuelle renseigner la date (le jour de 1 à 31)

pour les fréquences hebdomadaires renseigner le jour

dans tous les cas renseigner l'heure
(un scan régulier pendant l'heure de repas est une bonne habitude)

Il est utile de lancer une analyse de façon régulière afin de s'assurer que des virus ne soient pas sur votre ordinateur malgré toutes les précautions prises. La prolifération actuelle des virus et leur rapidité de transmission, permettent à certains virus ou chevaux de Troie de s'installer sur votre ordinateur avant que les concepteurs de logiciels antivirus ne trouvent la parade. Une analyse à posteriori de vos disque durs avec les mises à jour opérationnelles permet d'éradiquer les virus qui seraient passés au travers de l'antivirus.

En tout état de cause NE JAMAIS OUVRIR de fichiers dont vous ne connaissez pas la provenance ou sans vous être assuré auprès de l'expéditeur que c'est bien lui qui vous l'a envoyé. Les virus actuels récupèrent en effet les adresses mel des machines infectées et se propagent en usurpant les identités ainsi récupérées. Certains collègues ont reçus ainsi des mel avec des fichiers contenant des virus qu'ils s'étaient soi-disant envoyés !

7. Configuration de la mise à jour *(pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)*

Cliquer dans la case « Mise à jour » de l'écran d'accueil Trend Micro Internet Security

Cliquer sur le pavé « Paramètres de mise à jour », une boîte de dialogue s'ouvre.

Si vous êtes connecté directement via ADSL, choisir toutes les 3 heures.

Si vous êtes connecté en Numéris ou en RTC (ligne normale) il est préférable de faire les mises à jour de façon manuelle ou de les espacer pour économiser les coûts de connexion.

Si vous désirez avoir un message à chaque fois que l'antivirus est mis à jour, ne cochez pas la seconde case. (utile les premiers temps, fastidieux ensuite)

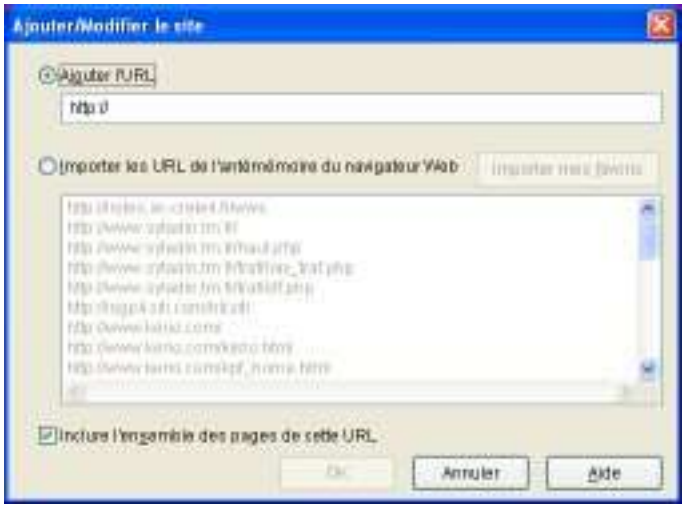
Pour les ordinateurs en réseau, passant par un proxy, renseigner les paramètres de la même manière que pour votre navigateur. Dans le cas d'un réseau d'établissement, la solution réseaux « OfficeScan » de Trend Micro est préférable à PC-cillin.

8. Activation du filtrage d'URL (d'adresses de sites Internet) *(*

pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)

Cliquer dans la case « Internet » de l'écran d'accueil Trend Micro Internet Security

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>Cliquer sur le pavé « Filtrage des URL », une boîte de dialogue s'ouvre.</td>
<td>Cocher la case « Activer le filtrage des URL »
Il est possible d'AUTORISER TOUTES LES ADRESSES, avec des exceptions
Il est possible de BLOQUER TOUTES LES ADRESSES, avec des exceptions
Selon l'alternative choisie, les exceptions peuvent être ajoutées, modifiées, supprimées (il s'agit des adresses de sites)</td>
</tr>
</table>



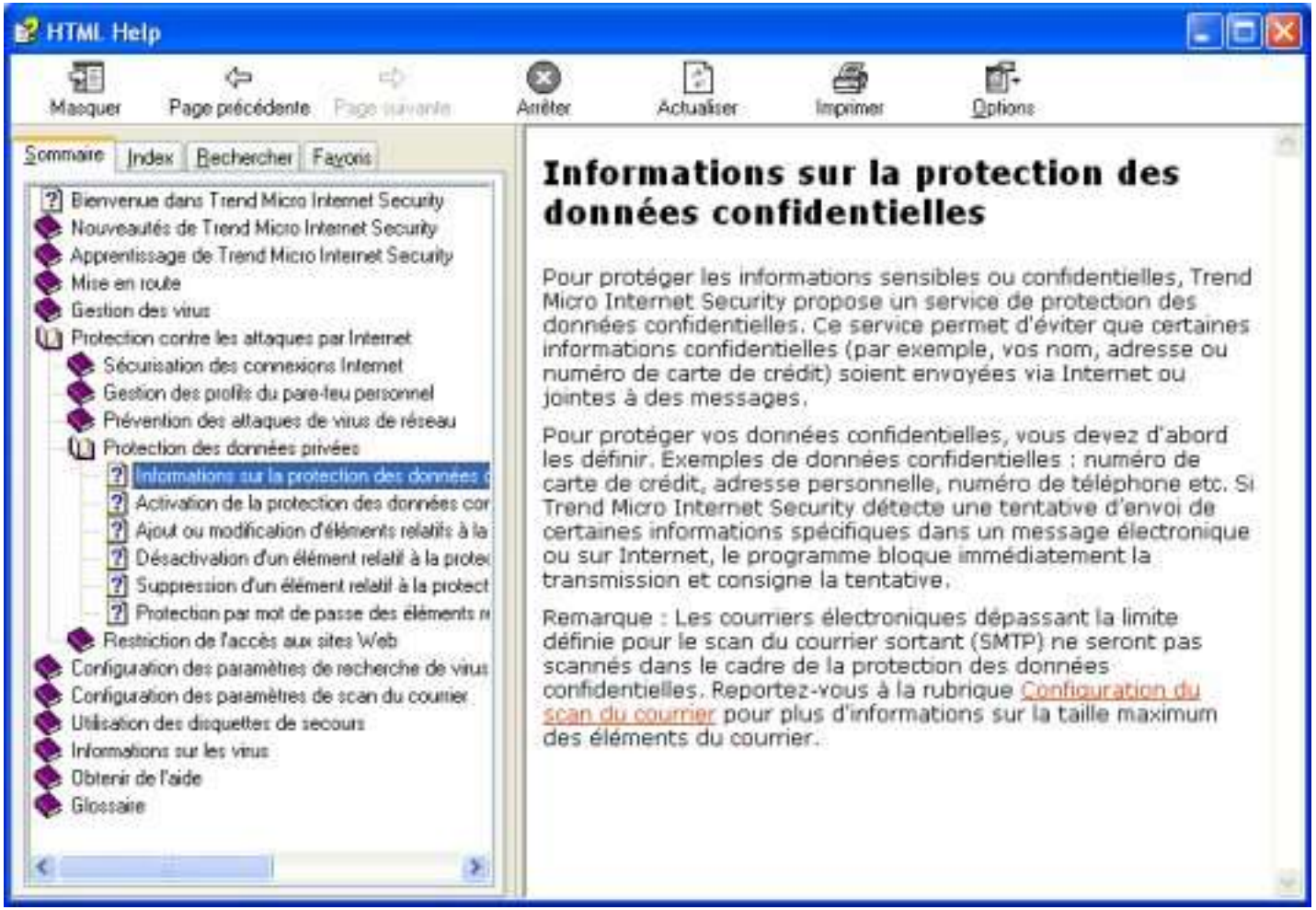
Il est possible d'ajouter les adresses (URL) une par une, de sélectionner celles que l'on vient de visiter (antémémoire du navigateur) et/ou de choisir l'ensemble des pages d'un site.

Dans le cas d'une interdiction (BLOQUER), le logiciel a déjà autorisé l'accès à ses propres sites, afin de permettre l'accès aux informations relatives aux virus.

9. Activation de la protection des données personnelles

(pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)

Cette fonction n'a pas encore été testée. Quelques extraits de l'aide de PC-cillin



Informations sur la protection des données confidentielles

Pour protéger les informations sensibles ou confidentielles, Trend Micro Internet Security propose un service de protection des données confidentielles. Ce service permet d'éviter que certaines informations confidentielles (par exemple, vos nom, adresse ou numéro de carte de crédit) soient envoyées via Internet ou jointes à des messages.

Pour protéger vos données confidentielles, vous devez d'abord les définir. Exemples de données confidentielles : numéro de carte de crédit, adresse personnelle, numéro de téléphone etc. Si Trend Micro Internet Security détecte une tentative d'envoi de certaines informations spécifiques dans un message électronique ou sur Internet, le programme bloque immédiatement la transmission et consigne la tentative.

Remarque : Les courriers électroniques dépassant la limite définie pour le scan du courrier sortant (SMTP) ne seront pas scannés dans le cadre de la protection des données confidentielles. Reportez-vous à la rubrique Configuration du scan du courrier pour plus d'informations sur la taille maximum des éléments du courrier.

Ajout ou modification d'éléments relatifs à la protection des données confidentielles

Pour pouvoir assurer la protection de vos données confidentielles, vous devez d'abord saisir ces dernières. Par défaut, Trend Micro Internet Security présente cinq champs pour les éléments de données, mais vous pouvez ajouter autant d'éléments que vous le souhaitez. Les cinq éléments préconfigurés sont : Nom, Carte de crédit, Numéro de téléphone, Nom de connexion et Mot de passe.

Remarque : Trend Micro vous recommande d'utiliser seulement des détails partiels pour les données telles que le numéro de carte de crédit ou le mot de passe. Par exemple, saisissez uniquement les quatre premiers chiffres de votre numéro de carte de crédit. Les données partielles sont suffisantes pour bloquer toute tentative d'envoi des données complètes. Il est également recommandé de définir un mot de passe pour protéger vos données confidentielles ; reportez-vous à la rubrique Protection par mot de passe des éléments relatifs à la protection des données confidentielles.

Pour ajouter ou modifier un élément relatif à la protection des données confidentielles :

1. Dans la fenêtre principale de Trend Micro Internet Security, cliquez sur **Internet > Protection des données confidentielles.**
2. Vérifiez que la case **Activer la protection des données confidentielles** est cochée.
3. Choisissez l'une des actions suivantes :
   - Pour ajouter un nouvel élément, cliquez sur **Ajouter**.
   - Pour modifier un élément existant, sélectionnez-le, puis cliquez sur **Modifier**.
4. Saisissez un nom et une description pour l'élément dans les champs **Nom de l'élément** et **Description**.
5. Entrez vos données confidentielles dans le champ **Données confidentielles**. Trend Micro Internet Security établit une correspondance exacte des données au moment où vous les saisissez. Notez que les informations que vous saisissez respectent la casse, ainsi *trend, TREND* et *tReNd* sont considérés comme des mots différents.
6. Choisissez l'une des actions suivantes :
   - Pour empêcher l'envoi de cet élément sur le Web, cochez la case **Vérifier le protocole Internet**.
   - Pour empêcher l'envoi de cet élément par e-mail, cochez la case **Vérifier le protocole de messagerie**.
1. Cliquez sur **OK**. L'élément est enregistré.

10.Activation d'un mot de passe pour la configuration des deux dernières fonctions (7 & 8)

(pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)

Cliquer dans la case « Internet » de l'écran d'accueil Trend Micro Internet Security

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>Cliquer sur le pavé « Mot de passe », une boîte de dialogue s'ouvre.</td>
<td>Cocher la case « Activer la protection par mot de passe »

La première fois renseigner uniquement les zones « Nouveau mot de passe » et « Confirmez le nouveau mot de passe »

Les fois suivantes, ne pas oublier de renseigner aussi la zone « Mot de passe actuel » avant de renseigner les zones modifiant le mot de passe pour en établir un nouveau.</td>
</tr>
</table>

11.Vérifier votre protection *(pour accéder à l'écran principal d'accueil du menu de configuration -voir page 2-)*

Cliquer dans la case « Etat » de l'écran d'accueil Trend Micro Internet Security

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>Cliquer sur le pavé « État de la sécurité internet », une boîte d'information s'ouvre.</td>
<td>Pour utilisateur avertis ; donne un certain nombre de renseignements et d'indications sur les modules activés ou non. Cliquer de nouveau sur la case « État » pour passer aux options suivantes.</td>
</tr>
</table>

Une fois cliqué sur le pavé « État antivirus », une boîte d'information s'ouvre.

Pour utilisateur avertis ; donne un certain nombre de renseignements et d'indications sur les modules activés ou non. Cliquer de nouveau sur la case « État » pour passer aux options suivantes.

Une fois cliqué sur le pavé « Journaux d'évennements », une boîte d'information s'ouvre.

Pour utilisateur avertis ou curieux : choisir le type de journal voulu, puis cliquer sur le pavé « Journaux ».

Sont consignés dans ces journaux les différentes actions du logiciel, ce que les informaticiens appellent les « log »