



# CASES articles

Les services de messagerie instantanée comportent des failles

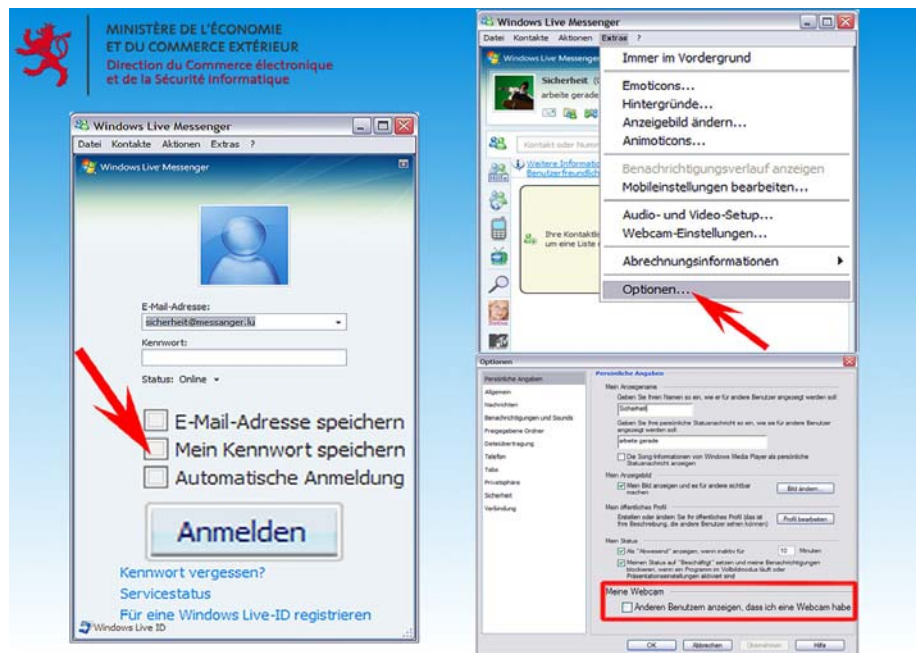
## Comment correctement configurer MSN Live Messenger

Pour plus de sécurité, adoptez les réflexes CASES !

Une vérification de la configuration permet d'améliorer la sécurité

Les services de messagerie instantanée sont devenus incontournables pour les enfants et les adolescents. Ils utilisent ces applications pour chatter par le biais d'Internet. De plus en plus d'adultes utilisent d'ailleurs ces services pour échanger des messages électroniques et des données. Cependant, rares sont les utilisateurs conscients des risques liés à ces services. La configuration standard même des applications de messagerie comporte ainsi des failles et permet aux cybercriminels de passer à l'attaque. Quelques manipulations de l'utilisateur sont toutefois suffisantes pour y remédier et ainsi réduire considérablement les risques de sécurité.

L'année scolaire 2007/2008 touche à sa fin. Dans la classe de 3<sup>e</sup> d'une école primaire au Luxembourg, le cours relatif à la sécurité de l'information a commencé. À la première question posée « Comment utilisez-vous Internet ? », une écolière répond sans hésiter « MSN », et elle explique que cela permet de dialoguer par Internet. Tous les autres enfants de la classe connaissent et utilisent également « MSN ». Rien de surprenant pour le responsable des cours, François Thill, du portail de sécurité luxembourgeois CASES : « De nos jours, enfants et adolescents utilisent les services de messagerie instantanée aussi naturellement que les téléphones mobiles. De



plus en plus d'adultes ont également recours à ces services, connus sous le nom de « MSN ». Toutefois, les enfants et les adolescents qui utilisent ces programmes ne sont guère conscients des risques et des dangers qu'ils peuvent dissimuler. Ceci est d'ailleurs également valable pour bon nombre d'adultes. Les statistiques démontrent pourtant que plus de 10 % des victimes des cybercriminels sont entrées en contact pour la première fois avec ces derniers par le biais de services de messagerie instantanée.

La communication et les échanges de données en temps réel grâce aux services de messagerie instantanée sont commodes et très populaires. Mais ces services ne sont pas sans failles : ils peuvent être utilisés dans un but malveillant par des tiers et donc comporter certains risques pour les usagers. Manque de confidentialité lors de l'échange d'informations et absence d'authentification de

### Conseil de sécurité Windows Live Messenger : messages

Si l'ordinateur privé est utilisé, l'utilisateur doit impérativement veiller à ce que les dialogues et données échangés soient sauvegardés. Ceux-ci peuvent en effet s'avérer utiles en tant que preuve lorsqu'il s'agit de dénoncer le comportement déplacé d'usagers d'Internet malintentionnés. Si le service de messagerie Windows Live Messenger est utilisé à partir de l'ordinateur privé, il convient donc de veiller à ce que l'option « Conserver automatiquement un historique de mes conversations » sous « Outils » et « Options » soit cochée. Cette fonction peut s'avérer utile lorsque l'utilisateur est confronté à du cyberharcèlement, du harcèlement sexuel ou à toute autre forme d'acte malveillant.

l'interlocuteur figurent parmi les failles connues de ces systèmes. La propagation de malwares par le biais de ces services ainsi que les harcèlements en tous genres et donc le mobbing électronique sont autant de risques auxquels s'exposent les utilisateurs.

Quelques gestes permettent pourtant de remédier à d'importantes failles de sécurité : il suffit pour l'utilisateur de modifier certains réglages de base grâce à des manipulations simples et rapides. Ceci permet de réduire efficacement les failles pouvant être exploitées par les cybercriminels et ainsi d'augmenter la sécurité.

### **Configurer Windows Live Messenger afin d'améliorer la sécurité**

Tout comme dans l'exemple décrivant la configuration de Windows Live Messenger suivant, les utilisateurs de messageries instantanées peuvent vérifier et éventuellement modifier les réglages de sécurité des programmes installés sur leur ordinateur. Ces réglages devraient d'ailleurs également être vérifiés chaque fois que l'utilisateur utilise un service de messagerie sur un ordinateur étranger.

La vérification commence dès le lancement du programme. Au démarrage de Windows Live Messenger, aucune des trois options suivantes ne devrait être cochée : « Mémoriser mon adresse », « Mémoriser mon mot de passe » et « Connexion automatique ». Cela permet de garantir que ni l'adresse e-mail, ni le mot de passe de l'utilisateur ne seront sauvegardés par l'ordinateur et qu'aucune connexion à Windows Live Messenger ne sera établie automatiquement, sans l'accord formel de l'utilisateur. Si un usager mémorise son mot de passe, celui-ci peut très bien être découvert par un pirate qui aurait par exemple réussi à s'introduire dans l'ordinateur par le biais d'Internet. Ceci est bien sûr

également valable pour toutes les personnes qui ont un accès physique à l'ordinateur en question. Le cybercriminel (ou toute autre personne) peut ensuite utiliser le service sous une fausse identité et par exemple harceler d'autres usagers. Les pirates espèrent également que l'obtention d'un mot de passe va leur faciliter l'accès au compte bancaire de l'utilisateur, de nombreuses personnes utilisent en effet le même mot de passe pour plusieurs applications.

D'autres réglages de Windows Live Messenger doivent être vérifiés. À cet effet, il convient de cliquer sur « Outils » dans la barre des menus de l'application puis sur « Options ». Les réglages des sous-menus suivants doivent être vérifiés : « Personnel », « Messages », « Dossiers de partage », « Transfert de fichiers », « Confidentialité », « Sécurité » et « Connexion ».

Si la barre des menus n'apparaît pas, celle-ci peut être affichée par l'utilisateur. Pour cela, il suffit de cliquer sur le bouton se situant le plus à droite dans le bandeau supérieur de la fenêtre de Windows Live Messenger et de sélectionner « Afficher la barre des menus ».

#### **Personnel**

Sous « Outils », « Options » et « Personnel », l'option « Indiquer aux autres utilisateurs que je dispose d'une webcam » devrait être décochée. Si cette option demeure activée, chaque personne qui s'entretient avec l'utilisateur par le biais de Windows Live Messenger saura que celui-ci dispose d'une webcam. Or, une personne malintentionnée peut infecter l'ordinateur à l'aide d'un cheval de Troie, activer la webcam pour ensuite prendre des photos à l'insu de l'utilisateur et les diffuser. Enfants et adolescents sont tout à fait capables de maîtriser les chevaux de Troie utilisés pour l'activation de webcams.

Sous « Enregistrer mes conversations dans ce dossier » peut être sélectionné un dossier pour l'enregistrement des conversations. Il convient toutefois d'être prudent avec cette option lorsque l'on utilise un ordinateur public, par exemple dans un cybercafé. L'utilisateur doit en effet se demander s'il est alors bien souhaitable d'enregistrer ses conversations, un éventuel accès à des contenus privés par des tiers ne pouvant être exclu. CASES recommande donc de décocher l'option « Conserver automatiquement un historique de mes conversations » lors de l'utilisation d'un ordinateur public, et de la cocher lorsqu'il s'agit de l'ordinateur privé.

Un guide de la configuration sécurité de Windows Live Messenger comportant de nombreuses captures d'écran est disponible sur le site [www.cases.lu](http://www.cases.lu), sous la rubrique « Publications » et dans le dossier « Sécurisation des messageries instantanées ».

#### **Dossiers de partage**

Cette option permet à l'utilisateur de partager des dossiers situés sur son ordinateur avec des contacts. Les contacts désignent alors les usagers d'un service de messagerie instantanée avec lesquels l'utilisateur échange des informations et des données. Chaque contact disposant des droits d'accès à un dossier particulier situé sur le disque dur de l'utilisateur peut y déposer des fichiers ou les lire. La liste des contacts ainsi que les droits d'accès accordés aux dossiers partagés devraient être soigneusement contrôlés par l'utilisateur. Cette voie peut en effet permettre aux malwares de se propager rapidement. Analyser les fichiers ainsi reçus à l'aide d'un programme anti-virus régulièrement mis à jour est donc indispensable. Lors de l'accès à des fichiers par plusieurs utilisateurs, il convient éga-

lement de tenir compte des éventuels droits d'auteur applicables.

Les droits d'accès peuvent être contrôlés par le biais du menu, en cliquant sur « Outils », « Options » et « Dossiers de partage ». L'utilisateur peut ainsi sélectionner les contacts pour lesquels il souhaite autoriser cette fonction. Dans le champ texte « Dossiers de partage » ne devraient figurer que des contacts bien connus de l'utilisateur. Tous les autres contacts y figurant devraient être effacés. Il convient également de vérifier que l'option suivante est bien décochée : « Quand je fais glisser un fichier vers le nom d'un contact, créer automatiquement un dossier de partage si ce contact n'en a pas encore ». Si cette option est cochée, il est nécessaire de la décocher.

Lorsque l'utilisateur reçoit une demande concernant le partage de fichiers, il devrait absolument vérifier l'identité du contact en question et son adresse e-mail. Le partage ne devrait être accepté que si l'utilisateur connaît le contact et lui fait confiance.

Les fichiers échangés par le biais de la fonction « Dossiers de partage » de Windows Live Messenger sont automatiquement enregistrés par l'ordinateur sur le disque dur C, dans un sous-dossier du dossier « Documents and Settings ». Les usagers utilisant un ordinateur étranger devraient tenir compte de ceci et il est recommandé d'effacer ces fichiers avant de quitter l'ordinateur en question. Il s'agit alors de ne pas omettre de vider également la corbeille de l'ordinateur étranger, les fichiers s'y trouvant peuvent en effet être restaurés aisément.

### **Transfert de fichiers**

Le menu « Outils », « Options », « Transfert de fichiers » permet d'accéder aux options relatives au « Transfert de fichiers ». Les options suivantes devraient être cochées : « Détecter les virus dans les fichiers

à l'aide de : » et « Rejeter automatiquement le transfert de fichiers pour les types de fichiers dangereux ». Le chemin vers le logiciel antivirus devrait être vérifié et éventuellement modifié en cliquant sur le bouton « Parcourir ». Une analyse anti-virus automatique des fichiers échangés est ainsi rendue possible. Il est alors bien sûr très important pour l'utilisateur de disposer d'un programme anti-virus régulièrement mis à jour.

La fonction « Partager automatiquement mes arrière-plans et accepter les arrière-plans partagés » devrait être désactivée et donc décochée.

### **Confidentialité**

Sous « Outils », « Options » et « Confidentialité », les fonctions « Autoriser seulement les contacts de ma liste verte à voir mon statut et à m'envoyer des messages » et « M'avertir lorsque quelqu'un m'ajoute à sa liste de contacts » devraient être cochées. Ceci permet d'empêcher que des personnes non autorisées puissent voir le statut de l'utilisateur et lui envoyer des messages. La liste verte ne devrait par conséquent comporter que des contacts dignes de confiance. Si un autre utilisateur souhaite ajouter l'usager à sa liste de contacts, une demande en ce sens est transmise à ce dernier. Il est recommandé de vérifier soigneusement ce genre de demande. Les services de messagerie instantanée sont en effet de plus en plus utilisés pour l'envoi d'e-mails indésirables – les spams. Les pirates utilisent ces services également pour la propagation de vers, ceux-ci se diffusant automatiquement par le biais des messageries instantanées. Les contacts indésirables peuvent être systématiquement bloqués à l'aide de ce menu. Il suffit de cliquer sur le contact devenu indésirable dans la « Liste verte » puis de cliquer sur « Bloquer » + « OK » pour le transférer dans la liste rouge et le bloquer.

### **Sécurité**

Le menu « Outils », « Options », « Sécurité » permet d'accéder aux options relatives à la « Sécurité ». Les trois fonctions suivantes devraient être activées dans ce menu : « Toujours demander mon mot de passe lors de la connexion à Hotmail, Windows Live Mail ou tout site compatible Windows Live ID », « J'utilise un ordinateur public : ne pas y stocker mon carnet d'adresses, mon image perso, ni mon message perso » et « Chiffrer les données de la liste des contacts pour qu'elles ne soient pas accessibles en dehors de Windows Live Messenger ». Ces fonctions permettent d'empêcher que la messagerie Hotmail soit lancée automatiquement à partir de Windows Live Messenger. Un pirate ayant éventuellement obtenu le contrôle de la messagerie instantanée ne pourra ainsi pas avoir automatiquement accès à l'application e-mail de l'utilisateur. Ces fonctions font également en sorte qu'aucune donnée personnelle, telle que le carnet d'adresses ou la photo de l'utilisateur par exemple, ne soit mémorisée sur l'ordinateur à l'issue de la cession de messagerie instantanée. Cela permet d'éviter de laisser des données personnelles lorsque l'on utilise un ordinateur étranger. De plus, la confidentialité de la liste des contacts est ainsi garantie : celle-ci reste confidentielle et ne peut être accédée en dehors de Windows Live Messenger.

Les deux fonctions suivantes devraient être désactivées : « Autoriser l'affichage des liens dans la fenêtre de conversation » et « Autoriser Windows Live Messenger à démarrer une conversation à partir d'un lien dans un navigateur Web ». Ceci permet par exemple d'éviter que des liens manipulés, menant vers des adresses indésirables, puissent être ajoutés dans la fenêtre de conversation par des pirates. Un lien éventuel n'apparaîtra dans la fenêtre de conversation que sous la forme d'une ligne de texte, celle-ci pouvant être,

le cas échéant, copiée vers la barre d'adresse du navigateur Internet par l'utilisateur.

### Connexion

Sous « Outils », « Options », « Connexion » et « Paramètres avancés », l'utilisateur devrait vérifier que la fonction « Conserver un journal de mes connexions au serveur pour faciliter la résolution des problèmes » est décochée. Cette fonc-

tion permet de remédier à d'éventuels problèmes de connexion. Lorsque cette fonction est activée, un fichier est sauvegardé sur l'ordinateur et si l'utilisateur oublie de l'effacer, une atteinte à la sécurité de l'ordinateur peut en résulter et des informations peuvent éventuellement être révélées.

Cette fonction devrait donc toujours être désactivée, sauf lorsqu'il s'agit de remédier à d'éventuels problèmes de connexion.

La vérification des différents réglages de Windows Live Messenger est simple et elle est fortement recommandée pour tout utilisateur, et en particulier pour les parents. Windows Live Messenger propose aux parents également d'autres fonctionnalités, destinées à la protection des enfants.

Les utilisateurs d'autres services de messagerie instantanée devraient également procéder à la vérification des fonctions et réglages décrits et présents dans leurs applications.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

[www.cases.lu](http://www.cases.lu)