



CASES articles

Un moyen de prise de contact apprécié des pirates :

Les messageries instantanées

Pour plus de sécurité, adoptez les réflexes CASES !

De nombreux dangers se cachent dans des systèmes tels que MSN ou ICQ

Les adolescents passent en moyenne plus de cinq heures par jour sur ce type de messageries

Que ce soit MSN, ICQ ou Yahoo Messenger, ces systèmes de messagerie instantanée permettent d'échanger, en temps réel, des messages électroniques ou des données avec les amis et les collègues. Les enfants et les adolescents sont tout particulièrement fascinés par ces nouveaux outils de communication. Chaque jour, ils sont en moyenne connectés plus de cinq heures à un système de messagerie instantanée. Ces moyens de communication si populaires dissimulent néanmoins bien des dangers, et la personne qui omet de s'informer ou qui n'applique aucun réflexe de sécurité peut aisément devenir la victime de cybercriminels.

Pour 2007, le rapport édité par le Centre américain de réclamations et de plaintes contre les délits sur internet (IC3) place les systèmes de messagerie instantanée à la quatrième place des moyens les plus populaires parmi les pirates, pour entrer en contact avec leurs victimes potentielles. Les avantages de ces systèmes de communication ne sont donc pas seulement appréciés des seuls usagers – les cybercriminels ne sont pas en reste. Le but des pirates étant d'attirer leurs victimes potentielles dans un piège.



Nombreux sont les utilisateurs qui ignorent tout des dangers que peuvent receler ces moyens de communication. Points faibles techniques et failles liées à une mauvaise utilisation des systèmes sont d'ailleurs tout aussi méconnus. De nombreux utilisateurs ne sont tout simplement pas conscients des importants préjudices qu'eux-mêmes ou des tiers peuvent subir de la part de pirates.

Des chiffres fournis par le prestataire de messagerie instantanée ICQ donnent un aperçu du nombre de victimes potentielles ainsi à la portée des cybercriminels : 400 millions de messages sont transmis quotidiennement par le biais de ce seul service. Chaque jour, l'utilisateur moyen demeure

connecté plus de 5 heures au système ICQ. 80 % de ces utilisateurs ont entre 13 et 29 ans.

Un utilisateur connaissant les dangers et les faiblesses du système peut aisément et rapidement adopter les réflexes de sécurité nécessaires. Outre les enfants et les adolescents, ce sont en particulier les entreprises et les parents qui ne maîtrisent pas complètement cet instrument de communication, qui devraient s'informer de son mode de fonctionnement et de ses dangers.

Comment fonctionnent les messageries instantanées ?

Contrairement au chat, les messageries instantanées constituent une variante de communication personnalisée, basée sur l'utilisation d'un ordinateur ou d'un téléphone mobile. Cela signifie normalement que les deux personnes ainsi en contact se connaissent mutuellement. L'échange des messages et des fichiers électroniques se fait en temps réel, tout comme pour le chat.

De petits logiciels, nommés messagers – tels qu'ICQ ou MSN Messenger – sont utilisés pour établir une liste des amis, des connaissances ou des contacts professionnels. Dès qu'une personne figurant sur cette liste est en ligne, cette information s'affiche sur l'écran de l'utilisateur. La communication est ensuite possible à tout moment.

À chaque utilisateur est attribué un numéro lors de son inscription. Dès que l'utilisateur est en ligne, son numéro est transmis à un serveur central. Celui-ci identifie le numéro et prévient les amis ainsi que les autres contacts figurant dans la liste que cet utilisateur est désormais en ligne. L'envoi de messages en temps réel peut ensuite commencer.

Ces services gratuits permettent de dialoguer tout en travaillant ou en faisant ses devoirs. Les enfants et les adolescents utilisent par exemple souvent l'ordinateur pour télécharger de la musique, jouer à un jeu et discuter avec plusieurs amis en utilisant une messagerie instantanée – le tout simultanément.

Les dangers liés à l'utilisation des messageries instantanées

La confidentialité n'est pas assurée

L'installation des applications de messagerie instantanée est généralement très simple – mais cette sim-

plicité génère certains risques : tous les messages échangés par le biais de ces applications sont transmis non cryptés via l'Internet. Les informations échangées entre collègues d'un même bureau transitent donc également par Internet. Cela signifie que la confidentialité des contenus et des fichiers ne peut être garantie. Les messages étant transmis en clair via le net, ils peuvent aisément être interceptés et altérés, sans que l'utilisateur s'en aperçoive. Le cryptage des données peut constituer une solution à ce problème, mais ce procédé n'a malheureusement pas été pris en considération lors du développement de nombreuses applications. Des programmes de cryptage peuvent toutefois être ajoutés sur différentes applications de messagerie instantanée. L'industrie propose en outre certaines solutions gratuites à l'utilisateur privé.

Un autre danger se dissimule dans les fonctions mêmes de ces applications. Celles-ci proposent par exemple de mémoriser le mot de passe de l'utilisateur. Mais cette mémorisation n'est bien souvent pas sécurisée et les utilisateurs devraient savoir que des outils permettant d'extraire les mots de passe des services de messagerie instantanée circulent sur la toile. Ces outils fonctionnent d'ailleurs même si le mot de passe est dissimulé sous ***** pour l'utilisateur. Quelques secondes peuvent suffire au cybercriminel pour obtenir un mot de passe.

Les usagers des messageries instantanées utilisant des ordinateurs publics, tels que ceux installés dans les cybercafés par exemple, ne peuvent pas savoir qui les a manipulés avant eux. Ces ordinateurs peuvent très bien contenir des programmes malveillants – comme des logiciels d'espionnage, destinés à intercepter les mots de passe. Par conséquent, l'utilisation d'ordinateurs publics pour des services de messagerie instantanée devrait absolument être évitée.

Conseil de sécurité

Un comportement adéquat et la mise en œuvre de mesures de protection techniques lors de l'utilisation des services de messagerie instantanée peuvent très sensiblement diminuer le risque de devenir la victime d'individus malintentionnés.

Le portail de sécurité de l'information luxembourgeois CASES (www.cases.lu) propose des informations précieuses quant à l'attitude et aux mesures de protection techniques qu'il convient d'adopter lors de l'utilisation des services de messagerie instantanée. Une liste détaillée des mesures de protection indispensables peut être consultée sous la rubrique « Publications », dans le dossier « Sécurisation des messageries instantanées ». Une des mesures qui y figurent porte sur le fait qu'un usager devrait utiliser un pseudonyme lors de son inscription à ces services. Ce pseudonyme devrait être choisi de manière à ne pas attirer l'attention d'individus malintentionnés. Le vrai nom ne doit jamais être communiqué, pas plus que le nom d'utilisateur et le mot de passe – y compris à des amis ou collègues de travail.

Dès que des cybercriminels sont en possession d'un mot de passe ou de données personnelles, ils peuvent usurper l'identité de l'utilisateur, faire du chantage ou porter atteinte à la réputation de ce même utilisateur.

Il convient également d'être prudent lors du raccordement de webcams à des services de messagerie instantanée. En exploitant d'éventuelles failles des services ou par le biais de malwares dissimulés sur l'ordinateur de la victime, des pirates peuvent par exemple activer la webcam d'un utilisateur et l'observer à son insu.

L'authentification n'est pas garantie

Une personne malveillante peut créer une identité fictive ou se faire passer pour quelqu'un d'autre grâce à un mot de passe volé. Un utilisateur ne peut donc jamais être certain que la personne avec laquelle il dialogue est bien celle qu'il pense. Une identité usurpée permet au délinquant de se présenter sous le nom de l'utilisateur auprès de ses amis, de ses connaissances ou de ses contacts professionnels. Cela peut porter préjudice à la réputation de l'utilisateur ou de tiers – ou pire. Les enfants et adolescents sont également confrontés à ce problème. Lors de formations sur la sécurité de l'information au profit d'enfants et d'adolescents luxembourgeois, dispensées en collaboration avec le Ministère de l'Éducation nationale et de la Formation professionnelle, l'équipe CASES a fréquemment rencontré ce genre d'abus : les enfants et adolescents confient souvent leurs mots de passe à leurs amis, ou utilisent des mots de passe très faciles à deviner. En cas de dispute, l'ancien ami se venge en se connectant à la messagerie instantanée en utilisant une fausse identité pour répandre mensonges, méchancetés et autres insultes.

Terrain de jeux pour virus, vers, canulars, lettres-chaînes et phishing

Les premiers vers se sont répandus via les messageries instantanées dès 2002. Les vers sont des malwares qui se propagent de façon autonome en utilisant les listes de contacts présentes sur les ordinateurs. Des mesures de protection techniques, comprenant la mise à jour régulière de tous les programmes, l'utilisation d'un anti-virus mis à jour quotidiennement ainsi que d'un pare-feu correctement paramétré, sont donc indispensables sur tout ordinateur utilisé pour des applications de messagerie instantanée.

Les mails-chaînes ou les canulars (catastrophes naturelles, alertes virus et autres actualisations de programmes anti-virus) se propagent rapidement et facilement par le biais des messageries instantanées. Ces messages sont généralement identifiables grâce à certaines caractéristiques : obligation de les transmettre à d'autres personnes, fautes d'orthographe, urgence, et même menaces à l'encontre du destinataire. Il est conseillé d'effacer purement et simplement ce genre de message.

Tout comme les sites de e-banking ou d'enchères en ligne, les services de messagerie instantanée sont des cibles privilégiées pour les phishers. Les cybercriminels essaient ainsi d'obtenir les données personnelles des utilisateurs. À cette fin, ils envoient des e-mails contrefaits, prétendant par exemple que le compte de messagerie instantanée de l'utilisateur a subi une attaque, et qu'il est nécessaire que l'utilisateur saisisse son mot de passe sur la page Internet du prestataire de messagerie, dont le lien figure dans le message. Les utilisateurs ainsi trompés sont dirigés vers une page Internet contrefaite par les pirates qui ressemble en tous points à la page originale. Si les victimes y introduisent leur mot de passe, celui-ci est intercepté par les pirates.

Rencontres dangereuses, pédophilie et cyberharcèlement

Les services de messagerie instantanée sont très populaires auprès des enfants et des adolescents, ce qui attire bien sûr les individus à tendance pédophile ou possédant d'autres orientations sexuelles. Des actes de harcèlement sexuel en résultent et les rencontres peuvent être d'autant plus dangereuses que l'utilisateur pense communiquer avec des amis et se sent en confiance. Des adultes ayant usurpé ou inventé une identité peuvent tromper leur interlocuteur. Les enfants et adoles-

Seuls des mots de passe assurant un niveau de sécurité acceptable doivent être utilisés. Ils ne doivent pas être faciles à deviner et devraient être changés fréquemment. De plus, un mot de passe différent devrait être utilisé pour chaque application. Les messages et les fichiers devraient être cryptés. Si cela devait s'avérer impossible, aucune information personnelle, ni données ou fichiers confidentiels ne devraient être transmis. Les ordinateurs publics ainsi que ceux partagés par plusieurs personnes ne devraient pas être utilisés pour les messageries instantanées. Il convient toujours de faire preuve de vigilance et de méfiance lors de la communication d'informations et de fichiers. Les contacts douteux ou indésirables devraient être bloqués. Des copies des messages échangés devraient alors être conservées en tant que preuve. L'ordinateur utilisé et les logiciels installés sur celui-ci doivent disposer des mises à jour les plus récentes. Un logiciel anti-virus ainsi qu'un pare-feu correctement paramétré sont indispensables. Avant toute utilisation des services de messagerie instantanée, les entreprises devraient procéder à une évaluation des risques et former leurs collaborateurs à une utilisation sécurisée de ces services. La bonne configuration du service de messagerie instantanée est d'une importance capitale. À cette fin, les utilisateurs peuvent consulter le dossier relatif à la sécurisation des messageries instantanées élaboré par CASES. Windows Live Messenger est utilisé en tant qu'exemple concret de messagerie dans ce dossier.

cents devraient donc toujours faire preuve de vigilance et de méfiance et ne jamais aller rencontrer des personnes dont ils ont fait la connaissance en chatant, sans être accompagnés de leurs parents.

Les services de messagerie instantanée sont également exploités pour le harcèlement, que l'on qualifie alors de cyberharcèlement ou cyberbul-

lying. Dans ce cas, les auteurs de ces méfaits peuvent aussi bien être des adultes, des adolescents que des enfants. Les conséquences pour les victimes peuvent être très graves et aller jusqu'à la volonté de s'ôter la vie. Si les auteurs de ces harcèlements sont des enfants, ils ne sont bien souvent pas conscients qu'ils commettent un délit et ignorent tout

des conséquences possibles pour leurs victimes, eux-mêmes ou leurs parents. Il est conseillé aux parents de partir à la découverte des messageries instantanées avec leurs enfants et de leur inculquer que les règles et normes sociales sont également valables pour l'Internet.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu