

Ne demandez rien, ne révélez rien OU D'accord, mais...

La question de la protection des mots de passe assurant l'accès au SIGNET-D est encore une fois à l'ordre du jour, les services opérationnels et les services de sécurité du Ministère voulant favoriser une meilleure conscience, à l'échelle globale, des raisons pour lesquelles cette question présente une telle importance.

Deux notions sont habituellement évoquées en rapport avec l'emploi des mots de passe, et la plupart des employés sont familiers avec la première de ces notions. Il s'agit de la protection de vos données, et donc des données ministérielles. Votre mot de passe vous permet de vous assurer que seules les personnes autorisées ont accès à ces données. L'autre notion, dont la connaissance est moins répandue, est que votre mot de passe établit de façon exclusive votre identité pour les fins du système, et contribue à l'intégrité de ce dernier en permettant de retracer les auteurs des activités accomplies au moyen du système. En d'autres mots, lorsque le système indique que vous avez effectué une opération donnée, la preuve en est apportée par le fait que votre code d'utilisateur et votre mot de passe ont été utilisés. Étant donné que le Ministère semble s'acheminer de plus en plus vers l'adoption de la messagerie électronique comme autre mode de communication officiel, il est crucial que nos systèmes soient d'une intégrité à toute épreuve.

Si je connais votre mot de passe, je peux accéder au réseau en usurpant votre identité et envoyer des messages électroniques sur n'importe quel sujet déplacé ou désagréable à quiconque au Ministère, comme je peux m'amuser à lire tout votre courrier électronique ou usurper votre identité pour envoyer un document confidentiel à la revue Frank, ou encore m'organiser pour accéder au SIGNET-D et effacer des blocs complets de données des serveurs. Je ne doute

pas que vous saisissez bien les données du problème.

Il y a plusieurs années de cela, le président des États-Unis, Bill Clinton, avait lancé un mot d'ordre sur une question militaire qui peut également s'appliquer à la question des mots de passe : ne demandez rien, ne révélez rien.

Du point de vue de la confidentialité, de l'intégrité et de l'accessibilité (les trois considérations principales en matière de sécurité informatique), il existe fort peu de raisons valables de jamais révéler à quiconque son mot de passe ou demander à autrui qu'il divulgue le sien. Extrêmement peu.

❶ D'accord, mais la personne avec laquelle je travaille m'a demandé de lui fournir mon mot de passe afin qu'elle puisse avoir accès à mes fichiers et à ma messagerie, au besoin, si je m'absente.

Ne demandez rien et ne révélez rien. Les messages électroniques importants qui ont trait aux activités de la direction doivent être adressés, tout comme les cc, au compte de votre direction et non à votre compte personnel. C'est d'ailleurs à pour cette raison qu'il existe des comptes organisationnels. Il importe que vos clients et vos correspondants soient conscients de ce fait. Par ailleurs, les fichiers qui présentent une importance pour la direction ne doivent pas être conservés dans votre unité personnelle H; ; à laquelle vous seul avez accès, mais dans le répertoire de la direction sur l'unité I: ou dans un répertoire de l'unité C: de votre poste de travail, afin de permettre à d'autres d'y avoir accès sans avoir à compromettre votre mot de passe. C'est pour cette raison que les unités I: ont été créées, et que votre poste de travail est doté d'une unité C.

ICONDESK est doté d'un dispositif limitant à 255 le nombre de messages que vous pouvez recevoir dans votre compte personnel (si vous vous absentez à l'occasion de vacances ou d'une affectation provisoire, ou pour toute autre raison), et en vertu duquel le système, une fois cette limite atteinte, renverra tout message subséquent à son auteur avec ce message mystérieux : « MTA Congestion ». Si vous ne recevez pas beaucoup de courrier électronique et qu'il vous est même impossible d'imaginer que 255 messages puissent s'accumuler dans votre compte, vous pouvez tout simplement vous organiser pour que votre courrier soit réexpédié à une autre personne. Consultez l'application ministérielle Profil ou communiquez avec l'administrateur des systèmes préposé au SIGNET-D pour obtenir des précisions à ce sujet. [Note de la rédaction : voir également l'article intitulé « Avant de partir en vacances : suggestion pour votre poste de travail » dans le n° 3 du bulletin *Connexions*, édition du 29 juillet 1996, pp. 9-10.]

Si, par contre, vous recevez généralement beaucoup de courrier électronique et qu'il est plausible que plus de 255 messages électroniques vous soient envoyés en votre absence, vous pouvez envisager de confier votre mot de passe à un collègue à qui vous faites totalement confiance. Si vous prenez cette décision exceptionnelle, nous ne pouvons trop insister sur l'importance de modifier votre mot de passe dès votre retour. [Note de la rédaction : ce qui précède constitue une modification par rapport aux recommandations fournies au point 2 de l'article intitulé « Qu'advient-il de vos messages en votre absence? », publié dans le bulletin *Connexions*, n°3, 29 juillet 1996, p. 5].

Veillez noter que cette limite de 255 messages ne s'applique pas

Suite en page 6 ►►►