



# Gérez vos mots de passe

Pour plus de sécurité, adoptez les réflexes CASES !

## Table des matières

1. Risques et conséquences
2. Comment gérer ses mots de passe ?

L'authentification par mot de passe est une des plus anciennes techniques de sécurité. Elle est toujours fortement utilisée et est considérée comme assez efficace si quelques règles fondamentales de sécurité sont respectées.

Lorsque vous allumez votre ordinateur, que vous souhaitez accéder à vos mails, que vous désirez vous rendre sur un site Internet privé ou consulter un fichier confidentiel, on vous demande la plupart du temps de donner votre mot de passe, on vous demande, en fait, de vous authentifier avant de pouvoir accéder à une ressource. Plus vous utilisez de services et plus vous surfez sur des sites Internet à accès restreints, plus vous êtes amenés à créer de nouveaux mots de passe et à vous en souvenir.



**Attention:** Utiliser un même mot de passe pour différents services, ordinateurs et sites Internet augmente les risques de se faire voler des informations personnelles et d'être victime d'usurpation d'identité.

Si l'un de vos mots de passe est découvert ou intercepté, tous vos mots de passe seront immédiatement corrompus.

Il est important d'assurer la sécurité de votre identité en suivant des règles de bonne conduite, en particulier celles relatives à la bonne gestion des mots de passe.



## Risques et conséquences

L'identifiant et le mot de passe associé sont très souvent le sésame vous permettant de vous annoncer et de décliner votre identité sur Internet, sur un ordinateur ou sur un service comme la messagerie ou la banque en ligne. Si un attaquant parvient à découvrir ou à le voler, il sera en mesure d'accéder à cet ordinateur ou ce service en se faisant passer pour vous : on parle alors

### EXEMPLE CONCRET

Imaginez que vous vous inscrivez à un forum parlant de jeux vidéo sur Internet. Il vous est demandé une adresse e-mail pour permettre la confirmation de l'inscription et un mot de passe pour sécuriser l'accès à ce forum. Vous vous dites que, pour simplifier la gestion de vos nombreuses identités électroniques et résoudre le problème de la multiplicité des mots de passe, vous allez utiliser votre mot de passe de messagerie pour accéder à ce forum. L'inscription s'est bien passée,

d'usurpation d'identité. Plus vous utilisez de services sur Internet, plus vous avez à vous souvenir de mots de passe et la tentation est grande de toujours utiliser le même pour se simplifier la vie, alléger sa mémoire et éviter les erreurs.

Quels sont alors les risques que vous encourez ?

vous êtes connecté sur le forum et êtes en mesure de discuter avec d'autres internautes.

Quelques jours plus tard, vous vous connectez sur votre messagerie : le contenu de votre carnet d'adresses et tous vos mails ont disparu. A la place, un seul et unique message laissé par le pirate : ce message est une demande de rançon, seul moyen pour récupérer vos mails et votre carnet d'adresses.

Mais au fait, que s'est-il passé ? Comment le pirate s'y est-il pris ?

## EXPLICATIONS

Lors de votre inscription sur le forum, vous ne pouviez pas savoir que son administrateur était au cœur d'un vaste réseau de vol d'identité. En réalité, le forum est un piège pour collecter, à l'insu des internautes, des mots de passe qui sont ensuite exploités pour perpétrer des actes illégaux, comme par exemple l'usurpation d'identité ou la demande de rançon.

Au moment de votre inscription, le mot de passe que vous choisissez est en réalité envoyé à des

pirates. Ceux-ci, sachant que les internautes utilisent souvent les mêmes mots de passe, parient sur le fait que parmi tous les internautes qui s'inscrivent, plusieurs d'entre eux choisiraient le même mot de passe que celui de leur messagerie. Puisque l'adresse e-mail est demandée au moment de l'inscription, il est donc facile de tester l'accès à la messagerie avec le mot de passe obtenu illicitement.

Les pirates parviennent ainsi à se connecter sur de nombreux comptes de messagerie et à mettre en œuvre leurs attaques.

## CONCLUSION

Cet exemple, qui reprend une situation très réelle, a pour objectif de vous rappeler que, dans certains cas, lorsque vous saisissez un mot de passe, vous ne pouvez être certain que votre interlocuteur est digne de confiance. Vous devez aussi vous méfier lorsque vous n'utilisez pas votre ordinateur, mais un ordinateur public. Dans ce cas, vous ne savez pas si les mots de passe que vous tapez ne sont pas enregistrés à l'aide de logiciels malicieux.

De plus, si le site Internet est mal sécurisé, il est possible qu'il soit la cible d'une attaque et que des pirates parviennent à voler les mots de passe des membres inscrits. De ce fait, si vous utilisez toujours le même mot de passe, vous risquez d'être la victime d'un vaste réseau de vol d'identité, suite à la corruption du site. Beaucoup de cas de figure existent où vous pouvez devenir victime d'un vol

d'identité. Protégez-vous contre ce risque et utilisez des mots de passe différents pour chaque service et veillez à ce que les mots de passe soient de bonne qualité. Des lois existent pour encadrer le bon usage des données personnelles des internautes. La Commission Nationale pour la Protection des Données, la CNPD, est garante de ces principes. Ainsi, il est important de rappeler que toutes les organisations qui gèrent des informations sur les personnes ont une obligation légale de protéger ces informations contre tout accès non autorisé et justifié.

Bien que l'obligation légale soit très stricte, il est essentiel que vous assuriez vous-même la protection de votre identité et de vos données personnelles. Une des premières étapes passe par l'application des règles de bonne pratique relatives aux mots de passe.



## Comment gérer ses mots de passe ?

### 7 REGLES DE BONNE PRATIQUE

Il est important d'assurer soi-même la protection de son identité et de ses données personnelles en suivant les 7 règles de bonne pratique suivantes:

1. **Changer les mots de passe par défaut**
2. **Longueur minimale de 8 signes**
3. **Simple à mémoriser mais complexe à découvrir**
4. **Ne pas réutiliser un mot de passe**
5. **Changer régulièrement de mot de passe**
6. **Le mot de passe est à usage personnel**
7. **Ne pas laisser son navigateur Internet gérer les mots de passe à sa place**



## PROPOSITION POUR LA GESTION DES MOTS DE PASSE

Niveau de confiance	Type d'information à protéger	Exemple de contexte	Spécifications du mot de passe
<b>0</b> bas	Aucune information spécifique à protéger  Mot de passe considéré comme restriction d'accès et non comme preuve d'identité	Site internet ne stockant aucune information personnelle  Site internet avec forum en ligne dédié à des sujets de loisir	6 caractères minimum Peut ne pas être changé
<b>1</b> moyen	Informations personnelle Mot de passe considéré comme preuve d'identité	Commerce en ligne sans conservation du numéro de carte bancaire  Messagerie / e-mail	8 caractères minimum Composé d'au moins 2 types de caractères Doit être changé au moins tous les 90 jours
<b>2</b> élevé	Informations sensibles Mot de passe considéré comme preuve d'identité	Banque en ligne  Commerce en ligne avec conservation du numéro de carte bancaire	8 caractères minimum Composé d'au moins 3 types de caractères Doit être changé au moins tous les 90 jours
<b>P</b>	Informations professionnelles	Contexte professionnel	Respecter la politique de sécurité par rapport à la longueur, la composition, les périodes de changement, les règles d'utilisation pour d'autres services de l'entreprise, etc...

### Trois exemples d'application de ce tableau :

1. Le code PIN à quatre chiffres d'une carte bancaire (niveau de confiance 2) est utilisé pour sécuriser des informations sensibles. Il ne serait pas correct d'utiliser ce même code pour une autre utilisation.
2. Le code PIN du téléphone mobile est utilisé pour en restreindre l'accès (niveau de confiance 0), de fait, le même code pourra être utilisé comme code d'ouverture d'une valise (niveau de confiance 0).
3. Un mot de passe pour accéder à un forum parlant des séries télé à la mode sur Internet (niveau de confiance 0) pourra être partagé entre plusieurs forums de loisirs sur Internet mais le mot de passe devra être différent de celui utilisé pour la messagerie électronique (niveau de confiance 1).

Retrouvez les dossiers, fiches thématiques, alertes et actualités sur :

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

CASES 2008