

Comment partager des identifiants et mot de passe de manière sécurisée

Bien que le partage d'identifiant reste une pratique marginale, il est parfois nécessaire d'envoyer - à nos prestataires notamment - des éléments de façon sécurisée. Découvrez comment le faire en respectant un minimum de sécurité

- [Introduction](#)
- [Rappel de quelques mauvaises pratiques à ÉVITER AU MAXIMUM](#)
- [1. Envoyer les accès par SMS, en deux temps, à deux numéros différents \(si possible\)](#)
- [2. Transmettre un mot de passe par voie orale: au téléphone \(si protégé\) ou en face-à-face](#)
- [3. Envoyer les accès par voie postale: envoyer les identifiants et mots de passe par lettre recommandée, si possible, en deux fois](#)
- [4. Utiliser une plateforme en ligne gratuite au chiffre et auto-détruit les messages après consultation](#)

Introduction

Avez-vous déjà envoyé des identifiants et mots de passe par email ou via chat d'entreprise? Si oui, sachez que cette méthode est très peu sécurisé, surtout si un jour un hacker prend le contrôle de votre boîte mail ou de votre ordinateur.

Dans cet article, vous allez voir 4 astuces qui vous permettront d'envoyer des mots de passe et identifiants de manière nettement plus sécurisée.

Rappel de quelques mauvaises pratiques à ÉVITER AU MAXIMUM

On l'a déjà tous fait au moins une fois mais voici un rappel de quelques **mauvaises pratiques à proscrire au maximum** lorsque l'on souhaite se rappeler d'un mot de passe ou l'envoyer à un partenaire, prestataire ou collègue de travail:

- Envoyer les accès et mots de passe par mail:

Si vous vous faites pirater votre boîte mail ou votre ordinateur, cela peut avoir de lourdes conséquences....

- Envoyer les accès par chat d'entreprise ou fil de discussion:

Sur n'importe quel terminal privé ou pro, ce n'est pas sécurisé.

- Écrire les accès sur un post-it (et les mettre sur votre bureau ou le bureau de la personne destinataire):

Ce que vous devez retenir, c'est que c'est complètement à proscrire...

1. Envoyer les accès par SMS, en deux temps, à deux numéros différents (si possible)

L'idéal, si vous souhaitez pouvoir **partager des accès de manière sécurisée rapidement** à une personne dans un environnement professionnel (ou personnel), c'est d'**envoyer les accès en deux temps par SMS et à deux numéros différents**:

- Envoyer l'**identifiant de connexion à un premier numéro** (ex: au numéro pro de l'intéressé).
- Envoyer le **mot de passe de connexion via un second SMS** à un autre numéro pro de préférence (ex: au responsable du destinataire).

Ainsi, si un des collaborateur de cette société (collectivité) se fait voler ou hacker son téléphone, le hacker n'aura que la moitié des accès et ne pourra donc pas en faire grand-chose. La probabilité que le hacker prenne le contrôle des deux téléphones concernés est nettement moins importante, le risque global est donc nettement limité.

2. Transmettre un mot de passe par voie orale: au téléphone (si protégé) ou en face-à-face

Éviter d'envoyer les accès par mail ou chat d'entreprise quand votre collègue est à 10 mètres de votre bureau.

Concernant le **partage des accès par téléphone**, le niveau de sécurité de cette action dépendra du niveau de sécurité des appareils mobiles ou fixes utilisés pour téléphoner mais cela reste une solution rapide lorsque les login / mot de passe ne sont pas trop sensibles et que les comptes sur les plateformes concernées sont eux aussi bien sécurisés (ex: comptes réseaux sociaux).

3. Envoyer les accès par voie postale: envoyer les identifiants et mots de passe par lettre recommandée, si possible, en deux fois

Vous n'êtes pas pressé par le temps? Cette astuce est globalement plus **sécurisée** et pourtant la moins utilisée car on souhaite tous obtenir les éléments à l'instant où nous les demandons...

Dans l'idéal, si vous souhaitez vraiment **transférer des accès de manière très sécurisée et surtout que vous avez une totale confiance dans le destinataire** et sur le fait qu'il détruira bien le papier une fois utilisé, envoyer les accès en deux temps par voie postale et, dans le meilleur des mondes, à deux adresses distinctes. Cette option est plutôt **bien sécurisée**.

4. Utiliser une plateforme en ligne gratuite au chiffre et auto-détruit les messages après consultation

Envoyer un lien sécurisé généré par OneTimeSecret ou 1ty à la personne de votre choix en lui communiquant le mot de passe pour l'ouvrir de préférence pas en même temps et pas par mail.

Moyen très sécurisé et rapide pour transmettre des identifiants ou mot de passe.

One Time Secret: