



# Comment sécuriser mes accès à Internet

Compte tenu de la vague de tentatives de piratage sur tous les supports : serveur, email, site Web, etc..., il nous semble utile de vous rappeler les règles élémentaires de sécurité.

La majorité du temps ce sont des tentatives pour essayer de subtiliser des informations confidentielles : carte bancaire, mot de passe.

**Voici quelques règles qu'il faudra respecter dans la mesure du possible concernant :**

## LES MAILS

- **si vous ne connaissez pas l'expéditeur**, n'ouvrez pas de mail, de pièce jointe, ne cliquez pas sur un lien situé dans le contenu,
- attention **aux mails de type "phishing"**, ce sont les imitations de mails officiels : CAF, impôts, banque, etc. Si vous n'êtes pas sûr(e), n'hésitez pas à contacter votre conseiller habituel. Sachez qu'aucun organisme ne vous demandera vos mots de passe ou informations confidentielles par mail,
- installez un **anti-virus activé** et à jour sur votre poste puis faites des contrôles de votre poste régulièrement,
- ne gardez pas de mail avec des informations confidentielles.

## LES MOTS DE PASSE

Tout d'abord, sachez qu'il est important d'**utiliser un mot de passe différent** pour chacun de vos comptes sur Internet. Ensuite, nous vous conseillons d'**utiliser des mots de passe ne contenant aucun mot existant**, mais plutôt une série de lettres, de chiffres et de caractères spéciaux.

### Comment sécuriser au mieux ses mots de passe ?

- Avoir des mots de passe de 12 caractères minimum, si possible de 16 caractères,
- Utiliser des caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux),
- Ne pas utiliser de mot de passe ayant un lien avec soi (noms, dates de naissance...),
- Le même mot de passe ne doit pas être utilisé pour des accès différents,
- Changer de mot de passe régulièrement,
- En règle générale, ne pas configurer les logiciels pour qu'ils retiennent les mots de passe,
- Éviter de stocker ses mots de passe dans un fichier ou lieu proche de **l'ordinateur**. Les mettre sur une clé USB ou un disque externe,
- Si possible, limiter le nombre de tentatives d'accès.

### Pour créer un mot de passe :

Vous pouvez tout à fait imaginer une phrase clé comme point de départ, comme par exemple « **Mon mot de passe est super bien sécurisé !** ».

En prenant la première lettre de chaque mot, en alternant les minuscules et les majuscules et en mettant des chiffres là où vous le pouvez, cela donnerait : « **MmDpEsbS1!** ».

Vous aurez alors un mot de passe unique, facile à retenir à partir d'un moyen mnémotechnique et surtout, difficile à pirater.

A titre d'exemple un mot de passe initialement choisi :

- **noumea** peut être cracké en **4 minutes !**
- **Noumea** peut être cracké en **7 minutes !**
- **Nouméa** peut être cracké en **3 heures !**
- **NoUméA** peut être cracké en **5 heures !**
- **NoUméA98800** peut être cracké en **33 années !**
- **#NoUméA98800#** peut être cracké en **33 siècles !**

## LA NAVIGATION SUR INTERNET

- Attention aux **sites sans certificat** : adresse en **http** au lieu de **https**. C'est le petit cadenas qui apparaît dans la barre d'adresse sur la majorité des sites. Si vous ne l'avez pas, soyez vigilant.  **https://**
- Méfiance sur **les réseaux wifi publics**, par ex : gare, restaurant, etc. Les informations transmises sur des sites non sécurisés peuvent être subtilisées par des personnes malveillantes