

COMMENT CRÉER UN BON MOT DE PASSE ?



CI-CERT

**CONTACTS:
CÔTE D'IVOIRE - COMPUTER
EMERGENCY RESPONSE TEAM**

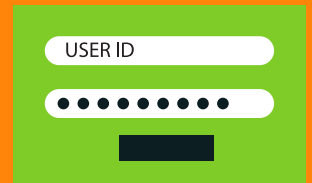
Tel : +225 20 34 43 73 / 74

Mail : info@cicert.ci

Site web : <http://www.cicert.ci/>

Marcory Anoumanbo, Abidjan – Côte d'Ivoire

SOMMAIRE



Introduction	3
Attitudes à proscrire.....	3
Critères pour un bon mot de passe.....	3
Alternative: utiliser une passphrase.....	4
Authentification à deux facteurs.....	4
Checklist.....	5



**CÔTE D'IVOIRE - COMPUTER
EMERGENCY RESPONSE TEAM**

Tel : +225 20 34 43 73 / 74

Mail : info@cicert.ci

Site web : <http://www.cicert.ci/>

Marcory Anoumanbo, Abidjan – Côte d'Ivoire

Introduction

Les mots de passe sont largement utilisés pour protéger l'accès aux renseignements professionnels ou personnels et aux outils en ligne, mais si les utilisateurs ne sont pas prudents, d'autres personnes peuvent utiliser leurs mots de passe afin d'accéder à des dossiers et à des renseignements cruciaux.

En effet, l'acquisition par des moyens « frauduleux » de mots de passe est la méthode classique la plus utilisée par les cybercriminels pour prendre le contrôle d'un système. De ce fait, choisir et sécuriser son mot de passe est principalement la mesure la plus importante à entreprendre.

Attitudes à proscrire

- Choisir les séquences de nombres simples, comme « 1234 » ;
- Utiliser des noms propres faciles à deviner, comme le prénom d'un enfant ;
- Avoir le même mot de passe pour plusieurs comptes ou systèmes.

Critères pour un bon mot de passe

- Choisissez des mots de passe comptant au moins huit caractères – plus le nombre de caractères est élevé, plus un mot de passe est sécuritaire ;
- Optez pour un mot de passe fort en incluant une combinaison des éléments suivants :
 - Lettres majuscules
 - Lettres minuscules
 - Chiffres ;
 - Caractères spéciaux (p. ex. : !, \$, # ou %)
- Gardez vos mots de passe confidentiels ;
- Changez vos mots de passe régulièrement (ex : tous les trois mois).



Alternative : utiliser une passphrase

Si vous avez besoin d'une sécurité renforcée, pensez à employer une phrase passe plutôt qu'un mot de passe. Il s'agit d'une phrase longue, difficile à "craquer", mais facile à retenir.

Au lieu d'utiliser un mot de passe garni de chiffres, de lettres mélangées et de symboles, il suffit donc de sélectionner des mots, qui forment ensemble une phrase. Ainsi, la phrase « **Je crée un mot de passe super sécurisé avec plus de 8 caractères et 4 types différents !** » deviendrait « **Jcumdps!Pd8ce4td!** »

Authentification à multiples facteurs

L'authentification à multiples facteurs est une pratique de sécurité qui ajoute un moyen d'identification supplémentaire, ce qui peut rendre le système d'une entreprise beaucoup plus sécuritaire.

Le « premier facteur » est une chose que la personne connaît (p. ex. un mot de passe) et le deuxième facteur est un élément à ajouter pour confirmer l'identité de la personne. Le deuxième facteur peut être une chose que possède l'utilisateur (p. ex. ses empreintes digitales, maintenant utilisées à de nombreux postes frontaliers) ou autre chose, comme un mot de passe à usage unique. À la différence du mot de passe ordinaire, le mot de passe à usage unique ne peut pas être deviné et, comme son nom le suggère, ne peut pas être utilisé à nouveau.

Le mot de passe à usage unique est généré par l'utilisateur avec une application sécuritaire (p. ex. son téléphone intelligent) ou un périphérique dédié (souvent appelé jeton). Les deux sont portatifs et peuvent être utilisés au besoin. Lorsqu'il est combiné à un nom d'utilisateur ordinaire et à un mot de passe, le mot de passe à usage unique renforce grandement la sécurité de l'authentification





Check-list



- ☐ Optez pour des mots de passe sûrs !
- ☐ Gardez vos mots de passe secrets !
- ☐ Utilisez un mot de passe pour chaque compte !
- ☐ Activez l'authentification à multiples facteurs si elle est proposée !



Test ton mot de passe

<https://password.kaspersky.com/fr/>



Veux-tu sauvegarder tes mots de passe

Utilises un gestionnaire de mot de passe
*par exemple : **KeePass** (Compatible avec toute plateforme)*



Côte d'Ivoire - Computer Emergency Response Team

Tel : +225 20 34 43 73 / 74

Mail : info@cicert.ci

Site web : <http://www.cicert.ci/>

Marcory Anoumanbo, Abidjan – Côte d'Ivoire