# Programmation

# Quelques conseils de sécurité

Il est trés important de prendre les précautions nécessaires afin d'empécher des intrusions de pirates ou l'utilisation de scripts nocifs qui pourraient non seulement permettre à un autre groupe d'individus de se connecter à votre compte et de modifier/télécharger/supprimer vos fichiers, mais aussi utiliser les ressources du serveur pour des buts illégaux (par exemple: envoi de SPAM).

Il est important de comprendre qu'en tant que titulaire d'un compte d'hébergement vous êtes ultimement responsable du contenu de votre compte. Il nous est impossible d'inspecter chaque fichier et chaque script envoyé sur nos serveurs afin d'en garantir la sécurité, et la responsabilité vous revient donc de bien faire votre recherche afin de vous assurez que tout script installé (surtout les scripts PHP) est :

- Sécurisé, c'est-à-dire qu'il n'a pas de failles de sécurité documentées sur Internet (une recherche Google incluant le nom de votre logiciel et le mot "vulnerability" pourrait vous éclaircir à ce sujet).
- Mis à jour. Il est important de toujours installer les versions les plus récentes des logiciels afin de bien avoir les corrections pour fermer les trous de sécurité dès que ceux-ci sont détectés. Des anciennes versions de logiciels sont souvent exploitables par des pirates à travers des trous de sécurités bien connus.
- Bien protégé par un mot de passe sécuritaire. Il vous est fortement recommandé d'utiliser un mot de passe avec plus de 8 caractéres, contenant des chiffres et des lettres, de ne pas utiliser le même mot de passe avec plusieurs services différents, et de changer les mots de passe régulièrement. Il faut bien insister sur ce dernier point. Un mot de passe non-sécurisé est la source de plus de 50% des intrusions de comptes, il est donc trés important d'utiliser un mot de passe trés robuste, surtout pour votre accés à cPanel et à vos bases de données.

D'autres astuces:

- Ne pas installer des scripts non-vérifiés par des professionnels, ou créés par des "amis ayant appris le PHP la semaine derniére". La programmation de scripts est chose facile à apprendre, mais difficile à maitriser. Il est fort probable qu'un novice ayant créé un script n'ait pas pris toutes les mesures nécessaires afin de garantir la sécurité d'un script.
- Toujours supprimer les répertoires d'installation de logiciels aprés leur installation, et ne pas laisser les fichiers avec des permissions 777 (qui peuvent être modifiés par tout le monde ayant accés au serveur).
- Ne pas afficher la liste de fichiers dans un répertoire sur votre compte d'hébergement (peut être désactivé via l'option à cet effet dans cPanel).
- Faire particuliérement attention avec les logiciels Joomla, Mambo, phpBB qui ont tous des failles de sécurité importantes dans leurs anciennes versions. Il faut donc réguliérement les mettre à jour.
- Faites des sauvegardes régulières de votre site web aprés chaque changement majeur. Si vous êtes piraté vous pourrez perdre des semaines,



**(c) 2026 Cyril <technique@archive-host.com> | 2026-11-12 18:03**

URL: http://docuwh.archive-host.net/index.php?action=artikel&cat=6&id=31&artlang=fr

voir des mois de travail. Il est vrai que nous effectuons des sauvegardes automatisées de votre compte à chaque jour, mais il est toujours préférable que vous ayez une copie locale (sur votre ordinateur) de tous les fichiers aussi stockés sur le serveur.
- Ne jamais dévoiler votre mot de passe de votre compte d'hébergement, et ne jamais l'envoyer par email.
- Dans les scripts que vous faites, n'ayez JAMAIS confiance dans les informations que peut donner un utilisateur. Vérifiez tous les champs.
- Certains logiciels espions peuvent s'installer sur votre ordinateur (par exemple si vous téléchargez un fichier envoyé dans un spam ou sur un site peu recommandable), ces logiciels recherchent un client FTP installés sur votre ordinateur, se connectent à votre compte et modifient les fichiers présents pour y mettre des virus ou pour infectés d'autres ordinateurs. La présence d'un antivirus sur votre ordinateur est nécessaire.

Référence ID de l'article : #1030
Auteur : Cyril
Dernière mise à jour : 2011-07-06 17:10


**(c) 2026 Cyril <technique@archive-host.com> | 2026-11-12 18:03**
URL: http://docuwh.archive-host.net/index.php?action=artikel&cat=6&id=31&artlang=fr