Bandeau:Protège-toi - Chiffre tes courriels

Protége-toi !

Le courriel est **une méthode de communication** décentralisé, et redoutablement efficace, inventé en 1965. Cependant, il ne s'occupe que de la transmission d'un message. Aucune sécurité du contenu n'a été prévu. De fait, les messages sont transmit en claire à travers le réseau internet. Cela signifie que le contenu est, à peu de chose près, aussi confidentiel que s'il était directement publié sur une page web. Le seul moyen de protection efficace pour garantir la confidentialité d'un courriel est le chiffrement de son contenu.

La seule la méthode que nous recommandons actuellement (en 2022) est le chiffrement asymétrique RSA (ou chiffrement à clef publique). Tu peux mettre en œuvre cette méthode en suivant, pas à pas, les explications donné ici : https://emailselfdefense.fsf.org/fr (voir aussi : https://gnupg.org/gph/fr/manual.html). Note que ce type de chiffrement sert non-seulement à **dissimuler un message**, mais aussi, et c'est très important, de **garantir l'identité de son émetteur**.

Ce sujet demanderait de longues explications, mais il faut retenir 3 choses :

1. La première chose qui est absolument essentiel et fondamental en matière de chiffrement, est que tu dois être le seul et unique maître de tes clefs. **Personne, absolument personne, ne doit avoir accès à ta clef privée !** Cela signifie que personne, appart toi-même, ne peut créer les clefs à ta place et que personne ne peux conserver ta clef privée à ta place. Si c'est le cas, il faut IMMEDIATEMENT révoquer ces clefs et en créer de nouvelles !
2. Une autre condition absolue pour la sécurité est que ton message doit être **chiffré sur TON ORDINATEUR** et n'être **déchiffré que PAR L'ORDINATEUR de ton correspondant**. Tu dois donc utiliser un “Client de messagerie” (pas de “messagerie web” ou “webmail”). Le client de messagerie **Mozilla Thunderbird** (https://www.thunderbird.net) est très bien adapté pour le chiffrement des courriels.
3. **Chiffre tous tes courriels**, même les plus anodins, lorsque tu échanges avec un correspondant qui a fournis sa clef publique. Vérifie que c'est effectivement la clef publique de ton correspondant (pour éviter les attaques de l'homme du milieu). En effet, si tu as un échange de 200 messages avec un correspondant et qu'il n'y a qu'un message chiffré dans le lot, il sera simple de savoir que ce message contient des choses importantes. Si tous les messages sont chiffrés, il sera impossible de localisé un message important et il sera impossible de savoir s'il y a même un message important dans ces échanges.

Une vérité à connaître lorsque l'on parle de chiffrement, c'est que quelque soit la méthode utilisée, le chiffrement ne garantit la confidentialité de son contenu que pendant un certain temps. Dans un avenir plus ou moins lointain, ces chiffrements seront cassable. Aujourd'hui, la plus grande menace sont les ordinateurs quantiques qui peuvent théoriquement casser toutes les méthodes de chiffrement actuelles ! Heureusement, dans les faits, ces ordinateurs sont actuellement incapable de le faire. L'élaboration d'une Cryptographie post-quantique est actuellement en développement.

Affaire à suivre...

Ne prend pas la sécurité –la tienne et celle de ton entourage– à la légère, surtout lorsqu'il s'agit d'informatique !

Description

Utilise ce bandeau en plaçant ce code dans la page :

```
{{page>:bandeau:protege-toi_-
_chiffre_tes_courriels&firstseconly&noheader&nofooter}}
{{tag>Bandeau:Protege-toi_-_chiffre_tes_courriels}}
```

Liste des pages qui utilisent ce bandeau

- FAL-VDT - Contact

Bandeau:Accueil