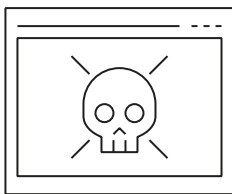


# Alerte aux rançongiciels

*Vos données en otage, contre de l'argent !*



*Vous êtes de plus en plus nombreux à recevoir des messages douteux avec des pièces jointes et/ou des liens qui sont piégés, **NE CLIQUEZ PAS DESSUS !***

Un virus pourrait chiffrer vos données et exiger une rançon. La payer ne garantit pas la récupération de l'intégralité de vos données.

Il est constaté de plus en plus d'**escroqueries** par des emails qui contiennent des pièces jointes et/ou des liens piégés. **Ces messages frauduleux sont maintenant plus difficiles à détecter** par les utilisateurs car ils sont bien souvent de parfaites copies, avec de vrais logos et sans faute d'orthographe.

## VOICI QUELQUES RÈGLES DE BON SENS QU'IL FAUT ABSOLUMENT RESPECTER :

*Ces réflexes sont indispensables et peuvent sauver votre entreprise !*



***N'ouvrez pas les messages dont la provenance ou la forme est douteuse.***

Aprenez à distinguer des emails piégés en deux minutes sur :

<https://www.hack-academy.fr/candidats/willy>



***Effectuez des sauvegardes régulières de vos données.***

Déplacez physiquement la sauvegarde de votre réseau et placez-la en lieu sûr.

Assurez-vous aussi qu'elle fonctionne.



***Mettez à jour vos principaux outils : Windows, antivirus, lecteur PDF, navigateur, etc.***

Et si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera la propagation des rançongiciels via les vulnérabilités des applications.



***Créer un compte « utilisateur » et n'utilisez que celui-ci, une fois votre ordinateur configuré.***

Cette règle ralentira l'escroc dans ses actions malveillantes.

Vous trouverez toutes les recommandations de l'ANSSI sur le site :

<http://ssi.gouv.fr>

En complément, il est recommandé de prendre quotidiennement connaissance des bulletins d'alerte du CERT-FR :

<http://www.cert.ssi.gouv.fr>

Si besoin, n'hésitez pas à solliciter vos prestataires informatiques sur ces sujets.

