

Reprise après cyberattaque (virus, ransomware, spyware...)

Les règles à appliquer sont les suivantes :

Vous avez subi une cyberattaque quelle qu'elle soit, infection par un virus via un système de mail ou de téléchargement ou après avoir été attaqué » par un ransomware (rançongiciel – logiciel cryptant votre disque dur, le déchiffrement étant obtenu contre paiement).

Votre système a été réparé.

Il vous faut maintenant :

- **modifier les mots de passe de vos différentes applications sur Internet** (courrier électronique – notamment webmails, messageries instantanées, réseaux sociaux, banque en ligne, FTP...), faites un effort au moins pour les applications qui vous paraissent les plus sensibles ;
- **effectuez une sauvegarde de informations** et astreignez vous par la suite à faire des sauvegardes régulières : de vos fichiers (entre **une fois par jour/semaine/mois**) ;
- **sauvegardez** également les **favoris/onglets/adresses de sites préférés** de vos navigateurs (google, mozilla, internet explorer) ainsi que **votre carnet d'adresses mails**.

Une **sauvegarde de votre système (une fois par an ou par semestre) est indispensable**. Elle est particulièrement utile si ce dernier est complexe à remonter. L'installation, en partant de zéro, d'un PC avec des applications de messagerie, applis bureautiques, un logiciel de sécurité, peut prendre plus de deux heures (beaucoup plus en cas de système complexe) et requiert en permanence un « opérateur », alors qu'une restauration ne prendra qu'une vingtaine de minutes et ne demande à l'opérateur que cinq minutes de son temps pour la lancer.

Si votre outil informatique est nécessaire à votre travail c'est d'autant plus important !