En cas de suspicion "d'attaque[1] informatique"

Phase de réaction immédiate :

1 – débranchez la prise réseau (internet) si vous êtes connecté en WiFi arrêtez le ;

2 - regroupez tous les supports (clef USB, disque dur externe…) qui auraient pu être utilisés sur cet ordinateur ;

3 laissez l'ordinateur fonctionner (le dépanneur que vous allez appeler voudra sans doute voir les symptômes de l'infection).

Phase de remise en état (par vous même ou par un spécialiste).

> Appel d'un spécialiste:

Prenez soin de noter tous les éléments qui permettront de décrire l'incident au dépanneur.

En cas d'appel, précisez notamment :

- le système d'exploitation (Windows 7, Mac, Linux…)
- les symptômes de l'attaque, quand s'est-elle produite ;
- ce qui d'après vous a pu la déclencher ;
- tout évènement simultané anormal : messages particuliers, sons, variation de luminosité de l'écran…

> Pour dépanner vous-même (temps 30 et 90 minutes, requiert un accès Internet et un autre PC) :

- pour les problèmes liés au navigateur télécharger l'application * AdwCleaner :

https://toolslib.net/downloads/viewdownload/1-adwcleaner/ et la lancer à partir du PC.

- pour les problèmes plus lié à une application installée sur le PC télécharger l'image de CD ROM Kaspersky Rescue Disk[2] : http://support.kaspersky.com/viruses/rescuedisk#downloads. Graver le CD et relancer la machine infectée avec le CD ROM (interactif).

Si vous avez Kaspersky, il est préférable dans ce cas de télécharger l'image CD ROM

D'Avira Rescue Disk à https://www.avira.com/en/downloads.

Attention aux attaques qui débouchent sur des chantages

Si un message vous demande de payer en ligne pour débloquer la situation ;

Si on vous demande de téléphoner pour contacter un technicien qui « débloquera la situation » ;

Si on vous demande de cliquer sur un bouton, ouvrir une pièce jointe, d'exécuter telle ou telle opération.
Ne le faites pas !

Au mieux vous appellerez un numéro surtaxé, au pire vous allez permettre au pirate de déployer son logiciel d'attaque et d'empirer la situation (destruction ou chiffrement de données, utilisation de votre PC pour commettre une attaque sur quelqu'un d'autre) et bien sûr récupérer un numéro de carte bancaire.

Les moyens pour se protéger d'une telle attaque sont les moyens de préventions (sauvegardes régulières). Il n'y a pas toujours de moyens curatifs, ils demandent du temps et coûtent cher.

1 Virus, comportement aberrant, impossibilité d'avoir accès à des ressources (fichiers, photos, réseau...) normalement présentes...

2 Il y a d'autres systèmes (trend micro, avira, f-prot…) qui proposent la même solution.