En cas d'attaque[1] ou suspicion d'attaque par voie numérique

(acte de cybermalveillance, tentative d'escroquerie, comportement visiblement anormal du terminal : affichage, ralentissement, perte d'informations…)
QUEL QUE SOIT LE MOYEN EMPLOYE (SMS, mail, réseau social, chat, téléphone…) EN CAS DE MESSAGE D'ALERTE, DE MENACE, DE PROPOSITION D'APPEL D'UN DEPANNAGE, **NE FAITES EN AUCUN CAS CE QUE LE MESSAGE DEMANDE DE FAIRE.**
Souvent un «dépanneur » appelle pour aller dans le sens du message.
Ne faites surtout pas ce qu'il vous demande, en revanche demandez lui poliment, de décliner son nom, son adresse et ses coordonnées et dîtes que vous le rappelerez en temps utiles.
Ces informations pourront être utile lors de l'investigation.

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 si vous décidez d'appeler un specialiste, laissez l'ordinateur fonctionner (le dépanneur que vous allez appeler voudra sans doute voir les symptômes de l'infection). Vous pouvez prendre une photo de l'écran pour lui communiquer.
Si vous avez payé quelque chose, f**aites immédiatement opposition** auprès de votre banque. Demandez le remboursement (Cela ne fonctionne pas dans la plupart des cas, mais certaines conditions le permettent parfois).

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 : message d'alerte inopiné avec ou sans alarme sonore

1 essayer de fermer le navigateur, s'il se ferme, passez directement à l'étape 4

2 Si le navigateur ne veut pas se fermer ou si le message réapparaît après fermeture : arrêtez l'ordinateur (ou le terminal, tablette, téléphone…). Si nécessaire forcez l'arrêt.

3 Attendez au moins une trentaine de seconde avant de le rallumer.

4 Relancez le navigateur

* Si le message a disparu alors videz le cache du navigateur (Ctrl + H ou Alt +H pour Firefox et effacez l'historique (choisir les options les plus complètes pour tout effacer). Fermez le navigateur, éteignez à nouveau votre ordinateur et attendre 30 secondes avant de le rallumer, puis relancer le navigateur. Logiquement le code malicieux qui permettait d'afficher le message a été supprimé.

* Si le message n'a pas disparu et qu'il reste bloquant, alors il faut désinstaller le navigateur. Pour ce faire, il faut recommencer les étapes 1 à 3, ne pas relancer le navigateur et désinstaller le navigateur. Si c'est Edge qui est bloqué, c'est un peu plus long. Sinon appeler un dépanneur.

5 Lancez un antivirus (vous pouvez utiliser celui préconisé ci-dessous). Lancer l'antivirus à demeurre sur l'ordinateur ne suffit pas, il vaut mieux en lancer un différent.
- pour les problèmes plus lié à une application installée sur le PC télécharger l'image de CD ROM d'Avira Rescue System à
https://support.avira.com/hc/fr/articles/360007776058-Créer-et-utiliser-Avira-Rescue-System.
Cette image peut s'installer sur un support USB. Il suffit après coup de le lancer et de suivre les indications.

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

Quelques remarques sur les différents modes d'attaque
Attention aux attaques qui débouchent sur des chantages par exemple déchiffrement du disque en échange d'une rançon, ou non divulgation de renseignements confidentiels
Dans tous les cas, ne jamais payer l'agresseur !

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 en aucun cas !
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.

Le site Cybermalveillance.fr donne différents scenarii d'attaque.
Les moyens pour se prémunir d'attaque sont essentiellement des moyens de préventions (sauvegardes régulières) qui permettent de repartir à moindre dommages. Face aux attaques, il n'y a pas toujours de moyens curatifs, et quand ils existent ils demandent du temps de mise en oeuvre et coûtent souvent cher.

Phase après l'attaque

Signalez les faits sur la plateforme du ministère de l'intérieur (Pharos).
Si vous avez été contacté par un faux support technique, signalez les faits sur la plateforme dédiée du ministère de l'Intérieur : Internet-signalement.gouv.fr.
Appel téléphonique de la plateforme info Escroqueries au 0 805 805 817

Déposez plainte
Au commissariat de police, à la brigade de gendarmerie ou au procureur de la République
Il est possible de se faire accompagner gratuitement par l'association France Victime 116 006 (service 7/7 09.00-19.00)

A la suite de toute attaque,
- changez vos mots de passe des mails, des sites d'achats en ligne ou de tout site de service.
- faites vérifier vos équipements.
Dans la majorité des cas, **il est plus sécurisant de réinstaller son système.**