Que faire si votre ordinateur ou smartphone est infecté par un virus ?

Pour un ordinateur (Windows, macOS, Linux)

1. **Choix d'un antivirus et un antimalware :** Avant de commencer, on choisie un antivirus et un antimalware fiables. Pour Windows, on peut opter pour des programmes populaires tels que Avast, Bitdefender, ou Malwarebytes. Pour macOS, on peut utiliser Avira ou Sophos, et pour Linux, ClamAV est un bon choix.
2. **Téléchargement des programmes :** On télécharge les dernières versions des programmes d'antivirus et d'antimalware depuis leurs sites officiels.
3. **Installation des programmes :** On suit les instructions d'installation pour chaque programme. On doit s'assurer de lire attentivement chaque étape et de décocher les options d'installation de logiciels supplémentaires si elles sont proposées.
4. **Mises à jour :** Une fois les programmes installés, on s'assure qu'ils sont à jour en recherchant les mises à jour depuis les paramètres de chaque logiciel.
5. **Analyse avec le logiciel antivirus :** On utilise l'antivirus installé et à jour pour effectuer une analyse complète du système. L'antivirus détectera et supprimera probablement la plupart des infections.
6. **Mises à jour système :** On s'assure que le système d'exploitation, le navigateur web et tous les logiciels sont à jour. Les mises à jour corrigent souvent les vulnérabilités exploitées par les virus.
7. **Examen des processus en cours :** Le gestionnaire des tâches permet d'examiner les processus en cours d'exécution. On recherche les processus suspects et on note leur nom.
8. **Utilisation du logiciels anti-malware :** On exécute le logiciel anti-malware pour rechercher et supprimer des logiciels malveillants spécifiques.
9. **Vérification des extensions du navigateur :** Dans le navigateur web, on désactive ou supprime toutes les extensions ou les modules complémentaires suspectés d'être à l'origine de l'infection.
10. **Changement de mots de passe :** On change tous les mots de passe, en particulier ceux des comptes sensibles, tels que les comptes bancaires et de messagerie, pour éviter une utilisation frauduleuse des informations.

Pour un smartphone ou une tablette (Android ou iOS) :

1. **Suppression des applications suspectes :** On désinstalle les applications récemment installées ou suspectes, en particulier celles provenant de sources non fiables.
2. **Mises à jour système:** On doit s'assurer que le système d'exploitation et les applications sont à jour en installant les mises à jour disponibles.
3. **Téléchargement d'une application antivirus/antimalware :** On accède au Google Play Store ou App Store (selon le système d'exploitation) et on recherche une application

antivirus telle que Bitdefender, Mobile Security ou Avast Antivirus. On télécharge et installe l'application choisie.

4. **Configuration de l'application :** On ouvre l'application et on suit les étapes de configuration initiale. Cela peut inclure la création d'un compte si nécessaire.
5. **Mises à jour antivirus/antimalware :** On doit s’assurer que l'application antivirus est à jour en téléchargeant les mises à jour depuis le Google Play Store ou App Store.
6. **Scan avec l’application anti-malware :** On utilise l’application anti-malware installée pour scanner et supprimer les menaces potentielles.
7. **Autorisations des applications :** On révise les autorisations accordées aux applications et révoquez celles qui semblent excessives ou suspectes.
8. **Gestion des comptes :** On doit changer les mots de passe des comptes, en particulier ceux liés à des applications sensibles comme les services bancaires en ligne.
9. **Réinitialisation de l'appareil :** En dernier recours, si le problème persiste, il faut envisager une réinitialisation de l’appareil aux paramètres d'usine pour supprimer complètement le virus.