Bonnes pratiques pour les utilisateurs contre les virus **(ces règles sont à prendre en compte en fonction du contexte) :**

1. **Faites des sauvegardes** : le risque virus ne peut être complètement réduit. En plus de limiter la propagation des virus, il faut également limiter l'impact des virus (en sauvegardant ce qu'ils peuvent détruire).
2. **Pas de panique** : les actions réalisées dans l'urgence font souvent plus de dégâts que les virus.
3. Faites une **analyse antivirus des supports amovibles** (clé usb, cdrom, disque dur externe, …) avant leur utilisation si elle n'est pas automatique.
4. **Supprimez les fichiers douteux sans les ouvrir**.

Un fichier douteux est un fichier ayant une **origine non sûre** :

- les **fichiers attachés** (**fichier en pièce jointe ou téléchargeable via un lien présent dans l'email)**, quelle qu'en soit l'expéditeur (vos amis vous envoient aussi des virus, puisque les virus utilisent leur carnet d'adresses),
- les **fichiers téléchargés** d'internet,
- les fichiers provenant d'une **clé usb**,

Un fichier douteux est aussi :

- un **fichier attaché que vous n'attendiez pas** (exemple : expéditeur inconnu, une facture sans avoir fait d'achat, une société commerciale qui ne vous écrit jamais, une offre d'emploi sans avoir déposé de CV, un expéditeur qui communique rarement avec vous, …),
- un **logiciel pirate** (crack de logiciel, logiciel de streaming illégal, …),
- un **fichier attaché exécutable** (.exe),
- un fichier attaché dont l'objet ou le texte de **l'email sont douteux**. D'une manière générale, il faut se méfier lorsqu'ils jouent sur vos affects, qu'ils exploitent l'actualité, qu'ils comportent des fautes d'orthographe ou qu'ils sont rédigés dans une langue étrangère (anglais, …).

5. Si le fichier vous parait douteux et qu'il vient d'un expéditeur connu, **demandez la confirmation** que le fichier attaché a bien été envoyé volontairement.
6. Préférez toujours échanger un texte saisi dans le corps du message plutôt que d'attacher une pièce jointe.
7. **Ne communiquez pas sur le risque ou l'infection.** Une mauvaise communication peut induire en erreur et avoir des répercutions négatives.
8. **Enregistrez la pièce jointe et ne l'exécutez pas depuis le logiciel de messagerie**. Les antivirus du poste de travail seront ainsi plus efficaces.
9. **Mettez à jour régulièrement votre antivirus** SAUF s'il est mis à jour automatiquement ou que vous n'avez pas accès à sa configuration.
10. **Mettez à jour vos systèmes d'exploitation et logiciels** SAUF s'ils sont mis à jour automatiquement ou que le fonctionnement de vos logiciels métiers dépend d'une version spécifique. Il s'agit plus d'**appliquer les correctifs de sécurité** que d'ajouter de nouvelles fonctionnalités.
11. Surveillez régulièrement les **signes d'alerte et d'erreur** provenant de votre antivirus ou de votre système d'exploitation. Appliquez l'action uniquement si elle vous paraît cohérente et en adéquation avec les règles définies ci-dessus.
12. **En cas de doute (sur la présence d'un virus ou pour appliquer les recommandations)**, faites appel à votre assistance de proximité.