

1. Présentez à vos utilisateurs les formats de fichiers qui peuvent être dangereux sur un PC (Windows, Linux, Mac), sur un smartphone ou une tablette (Android, IOS).

Les formats de fichiers sur pc sont .exe, .docx,
Et .apk et .xlsx qui peut etre dangereux sur smartphone.

2. Déterminez si des formats de fichiers sont plus dangereux que d'autres.

Argumentez.

Certains formats sont plus dangereux que d'autres car certains peuvent contenir des virus, des vers ou d'autres types de programmes malveillants.

3. Y a t-il des sources plus sûres que d'autres ? Explicitez avec des exemples.

Oui certaines sources sont plus sûres que d'autres comme par exemples:

- Les sites du gouvernement
- Les sites de officiels
- Les sites média reconnus

4.Comment allez-vous inciter vos utilisateurs à se protéger des menaces

Informatiques, dans notre cas d'un rançongiciel ?

Un rançongiciel : Programme malveillant qui chiffre les données personnelles de quelle qu'un dans le but de lui extorquer de l'argent.

Afin de se protéger nous pouvons effectuer plusieurs actions contre un rançongiciel comme :

- Effectuez des sauvegardes régulières de vos données sur un disque dur externe ou un cloud.
- Ne pas ouvrir les liens ou les messages qui ont une forme douteuse
- Mettre à jour vos outils principaux (mail , word, etc...)
- Utiliser un compte utilisateur.

5. Vos utilisateurs vont certainement vous prendre pour un « parano ».

Comment allez-vous démontrer que ces mesures peuvent être vitales pour

le bon fonctionnement de l'entreprise ?

Nous pourrions par exemple leur donner des cas concrets d'entreprise qui ont subi ce genre d'attaque en leur précisant les conséquences qu'on subit les entreprises donner dans les exemples en parlant des aspects financiers et des données potentiellement récupérer par le potentiel hacker.



