Bozion

Ugo

TSIO1

Respect des bonnes pratiques

1)Sur un pc il y'a plusieurs types de fichiers qui peuvent être dangereux, tout d'abord il y'a les fichiers .exe qui sont dangereux car ils peuvent contenir dans leur code source des instructions susceptibles de nuire à votre pc. Les fichiers .docx et .xlsx car ils peuvent comporter des macros malveillantes. Les fichiers html peuvent également être nuisibles car ils peuvent contenir du phishing. Les fichiers javascript peuvent exécuter des fichiers malveillants donc ils peuvent potentiellement être dangereux.

Pour les Mac il faut faire attention aux fichiers .app qui sont des applications qui peuvent donc être nuisibles si on installe les mauvaises applications.

Les fichiers .rar et .zip sont potentiellement nuisibles également car ils contiennent eux même d'autres fichiers.

Sur un téléphone Android, les fichiers .apk sont potentiellement dangereux car ils installent une application sur la machine et ils peuvent être infectés par un virus.

Sur les IPhone, il faut faire attention aux fichiers d'installation de manière comme les .ipa car on peut possiblement installer quelque chose de nocif pour notre appareil.

2) De manière générale les fichiers les plus dangereux sont les fichiers d'installation car ils vont installer un programme sur la machine qui peuvent être nuisibles à la machine, les fichiers les plus dangereux sont donc les .exe, les apk, les .app, les .ipa.

3) Il y'a des sources plus sûres que d'autres, si on souhaite installer un logiciel ou même de manière générale télécharger quelque chose sur internet, il faut d'abord vérifiez d'être sur un site sécurisé, avec un lien "https" au début et non "http", il faut toujours télécharger sur les sites officiels et non sur des sites

extérieurs, exemple, si on souhaite installer office, il faudra se rendre sur le second lien qui est le site officiel de Microsoft qui détient la propriété d'office et non sur le premier qui est un site tiers qui peut contenir par conséquent des fichiers malveillants

Il faut également ne pas télécharger les fichiers qui pourraient être envoyées par mail ou par quelconque moyen qui ne vient pas du site officiel du logiciel.

4) Un rançongiciel est un programme malveillant plus communément appelé virus qui verrouille l'ordinateur et ses fichiers en demandant le paiement d'une rançon pour les rendre disponibles. Un rançongiciel peut infecter une machine dès l'ouverture d'une pièce jointe où en naviguant sur des sites compromis. il faut donc prévenir les utilisateurs de l'existence de ce type de programmes malveillants et il faut également les initier aux bonnes pratiques de manière générale comme de sauvegarder régulièrement ses données pour pouvoir les récupérer en cas d'infection, ne pas cliquer sur les liens venants d'expéditeurs inconnus, ne pas installer d'application ne venant pas de sources sures cités précédemment et ne pas naviguer sur les sites illicites ou non surs de manière générale qui peuvent être nocifs.

5) Pour que les utilisateurs respectent les instructions et consignes que je leur aurait donné je leur expliquerait qu'un rançongiciel peut infecter la machine avec une simple pièce jointe dans un mail et neutraliser la machine mais surtout toutes les données qu'elle contient et je leur expliquerait que le coût direct moyen d'une cyberattaque réussie en

France est estimé a 25 600€ et 64 000€ pour les grandes entreprises, s'ajoutent à ça le coût de la rançon qui est en moyenne de 25 700€. J'expliquerais donc que de simples règles de précautions peuvent éviter à l'entreprise de payer de grandes sommes et que le simple fait de ne pas cliquer sur n'importe quel lien par exemple peut préserver l'entreprise de lourdes dépenses