RÈGLES D'HYGIÈNE CYBERNÉTIQUE

Sommaire

I. QU'EST-CE QU'UNE CYBERATTAQUE ?

1) Qu'est ce qu'une cyberattaque ?

Une cyberattaque est un acte offensif envers un dispositif informatique à travers un réseau cybernétique. Une cyberattaque peut émaner de personnes isolées ou d'un groupe de pirates informatiques, éventuellement étatiques.

2) Quelles sont les conséquences d'une cyberattaque ?

Une cyberattaque peut entraîner une cybercrise, que ce soit au niveau financier ou de réputation (les données utilisateurs risquent d'être exposées). Les cyberattaques peuvent entraîner les conséquences suivantes : blocage d'un site, vol d'identité, fraude, extorsion.

3) Quelques exemples de cyberattaques

→ **Cyberattaque de l'hôpital de Corbeil-Essonnes :** Le 23 septembre dernier, les hackers qui avaient attaqué l'hôpital de Corbeil-Essonnes, ont divulgué sur le darknet une partie des données piratées. Selon la cellule investigation de Radio France qui a pu les consulter, il s'agit d'informations très personnelles.

→ **Le géant de la viande JBS a été la cible d'une cyberattaque :** Le groupe a découvert que plusieurs des serveurs sur lesquels sont basés leur système informatique en Amérique du Nord et en Australie ont été visés par des *pirates informatiques*, sans préciser la nature de l'intrusion. Cette cyberattaque a causé une suspension des activités du groupe en Australie et de certaines lignes de production aux USA. JBS a finalement payé une rançon de 11 millions de dollars.

→ **Mairies de Annecy, Angers, La Rochelle…** Le nombre de cyberattaques contre les mairies et institutions locales a augmenté dès le début de l'année 2021. Ces villes ont signalé avoir été victimes de *tentatives d'extorsion de fonds* à la suite de l'introduction d'un logiciel malveillant dans le système informatique. Ces événements rappellent que les multinationales ne sont pas les uniques cibles des cyberattaques. Si les entreprises de grande taille restent celles qui sont les plus susceptibles d'être touchées, les petites entreprises de 10 à 49 salariés semblent particulièrement sensibles à *la vulnérabilité des serveurs ou au piratage d'identifiants.*

4) Comment se protéger ?

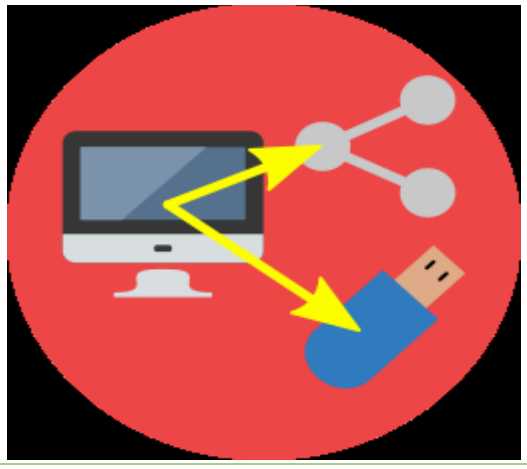
Dans notre vie personnelle comme dans notre vie professionnelle, nous utilisons de plus en plus d'outils informatiques (que ce soit sur ordinateur ou Smartphone) qui sont à la merci des cyberattaquants. Nous devons tous nous protéger pour réduire au maximum les conséquences de ces cyberattaques, en respectant quelques « règles d'hygiène informatique » et notamment grâce à des bonnes pratiques de sécurité.

II. EXEMPLES DE BONNES PRATIQUES DE SECURITE INFORMATIQUE

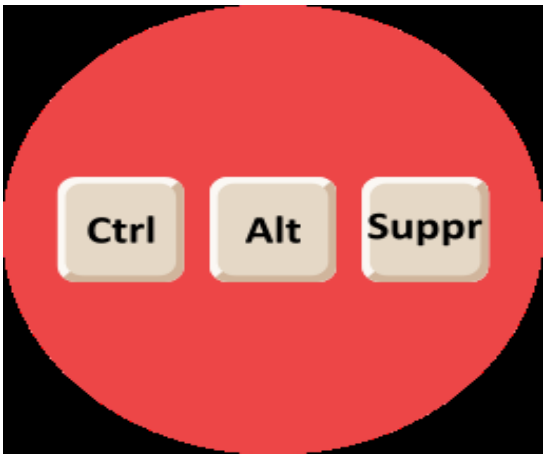
1) Exploitation du poste de travail

✓ Interdiction de connecter un équipement personnel à son poste de travail.

✓ Sauvegarder ses données sur un disque externe ou une clef USB fournie par l'administration.



✓ Verrouillage de son poste de travail obligatoire en cas d'absence.



2) Utilisation de la messagerie

✓ Ne pas faire confiance aveuglement à l'adresse de l'expéditeur.

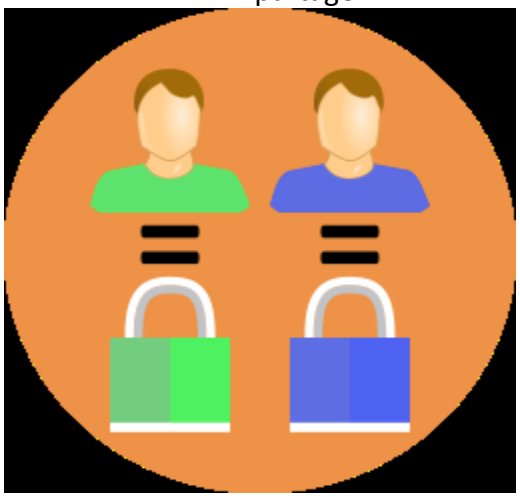
✓ Réfléchir avant de cliquer sur une pièce jointe.

✓ Interdiction d'utiliser une adresse électronique personnelle à des fins professionnelles.

✓ Demander confirmation en cas de doute sur un courriel.

3) Gestion des mots de passe

✓ Un mot de passe est personnel, il engage la responsabilité et ne doit pas être partagé.



✓ Un mot de passe doit être robuste et ne doit pas être utilisé sur plusieurs systèmes.

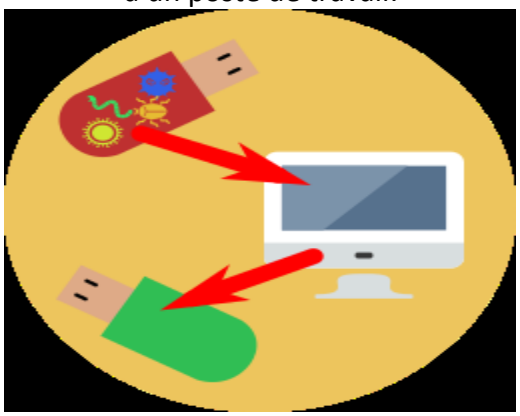
Interdiction de conserver ses mots de passe dans un fichier ou sur un post-it.

Interdiction de préenregistrer les mots de passe dans son navigateur.

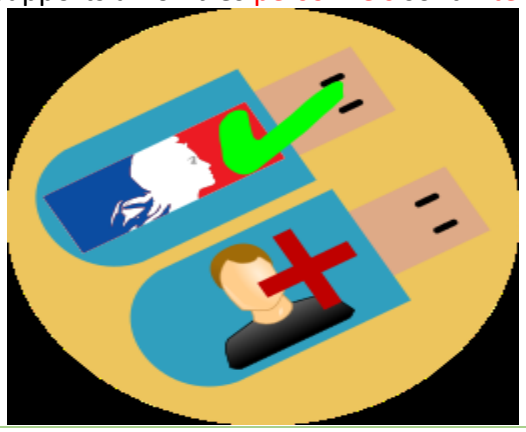
4) Utilisation des supports amovibles

Seuls les supports amovibles fournis par l'administration sont autorisés.

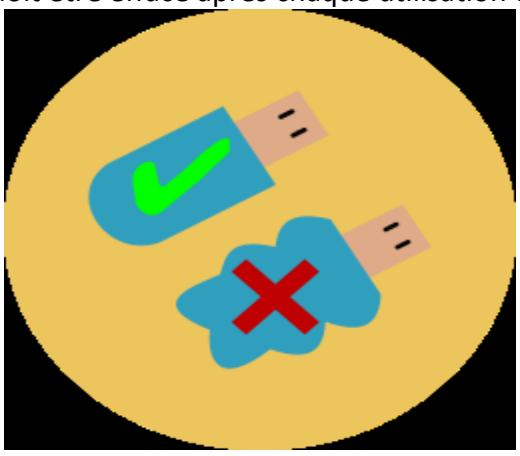
Un support amovible doit être décontaminé sur une station blanche [1]avant d'être connecté à un poste de travail.



Les supports amovibles personnels sont interdits.



Dans le cas où un support amovible est un moyen de transport contenant des données personnelles, il doit être effacé après chaque utilisation et conservé vide.



[1] *Station blanche : Ordinateur dédié pour tester les fichiers sur un support amovible dans le but de détecter les virus avant qu'ils ne soient autorisés à être utilisés avec d'autres ordinateurs*