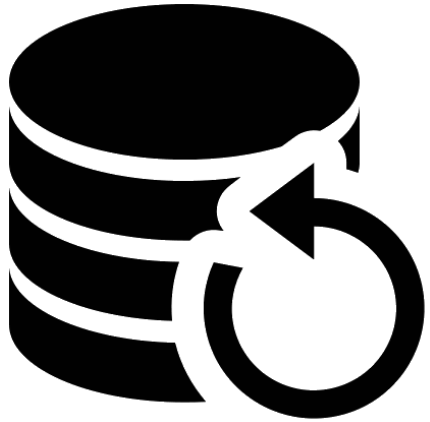
Florentin Bracq- -Flabat BTS SIO 1

TP 2 BYOD

Liste d’outils pour sécuriser un poste informatique

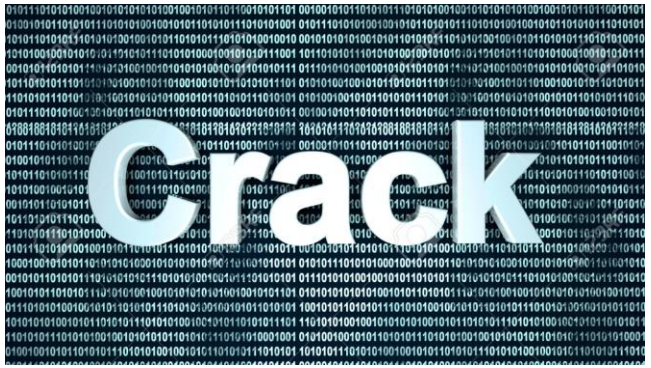
- Un antivirus en cours d’exécution et à jour
- Un pare feu activé
- Un anti-malware à jour et en cours de fonctionnement
- Un logiciel de sauvegarde installé et en cours d’exécution

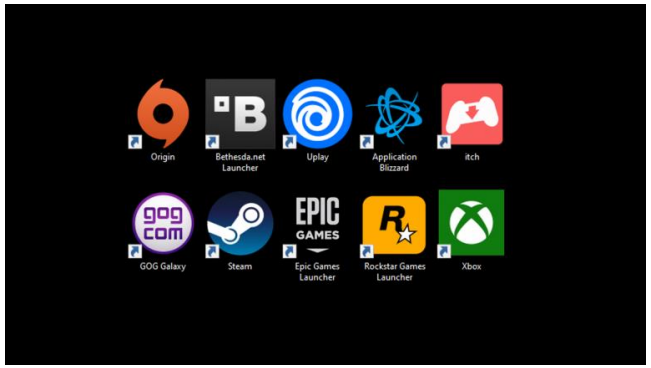


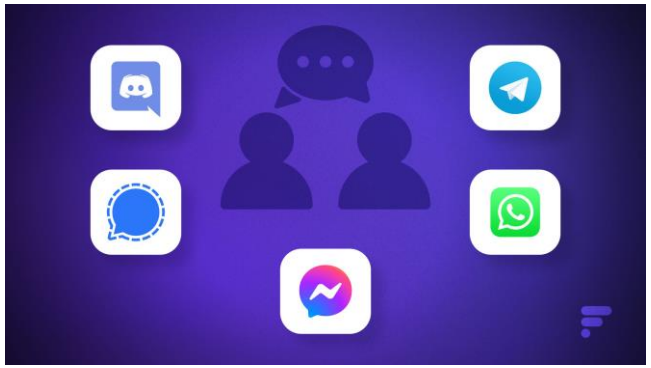



Liste d’outils ou logiciels interdits

- Des logiciels sous une licence personnelle pour un usage professionnel
- Des logiciels payants crackés
- Des jeux
- Des services de messagerie instantané personnels tels que Discord

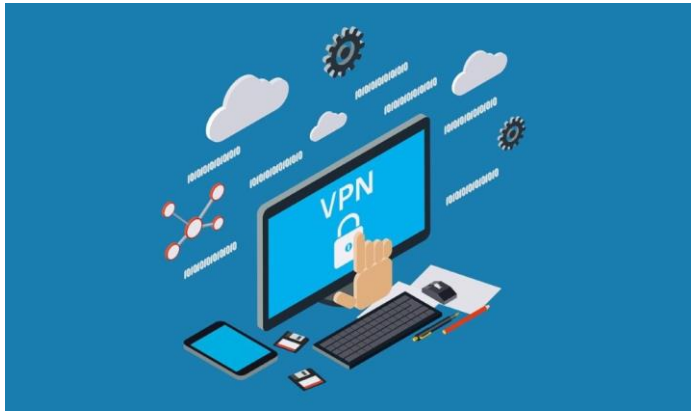






Outils de communication utilisés sur les postes informatiques

- Une connexion VPN pour accéder au réseau local de l'entreprise
- Microsoft Teams (outil de travail collaboratif)



Microsoft Teams

Politique de sécurité de mots de passe sur les postes informatiques

- Pour permettre une meilleure sécurité, il est important d'utiliser des mots de passe différents pour chaque compte en ligne. Si le PC est dans un domaine active directory, il est possible qu'il y ait une stratégie de mot de passe qui soit déjà en place, notamment par exemple un changement de mot de passe tous les mois.
- Lien d'un article de la CNIL sur les mots de passe :
- https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite

Comment sensibiliser les utilisateurs à l’usage du BYOD ?

- Il est possible de sensibiliser les utilisateurs à l’usage du BYOD, en faisant des interventions au sein de l’entreprise, ou encore en montrant une infiltration par un malware venant d’un PC personnel. Faire des spots vidéo de sensibilisation et des documents de sensibilisations

Bonnes pratiques personnelles et professionnelle

- Il y a des différences entre un usage personnel et professionnel d'un PC, pour un usage professionnel il faut prendre plus de précautions, notamment par rapport aux pièces jointes dans les mails, ou encore les périphériques de stockage inconnus.