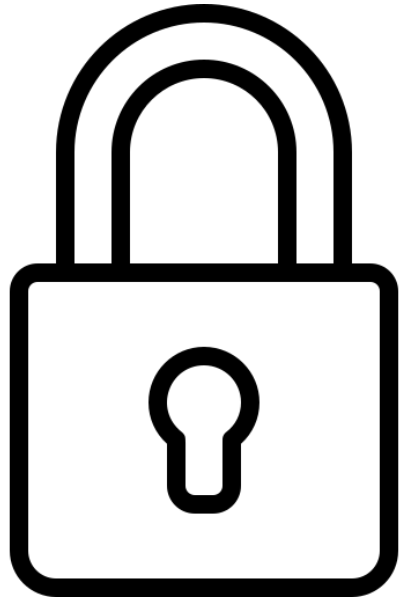
MISE EN PLACE DES BONNES PRATIQUES BYOD

OUTILS DE SÉCURITÉ A UTILISER

- Bloqueur d'appareil : Des personnes malveillantes pourraient se connecter au réseau grâce à ces appareils qui seraient non contrôlés
- Charte : mettre au clair les responsabilités des utilisateurs
- Séparer usages personnels et professionnels : créer compte distincts pour une même application
- Sécuriser les mots de passe : mots de passe administrateur réseau, mots de passe sur les sites etc ...

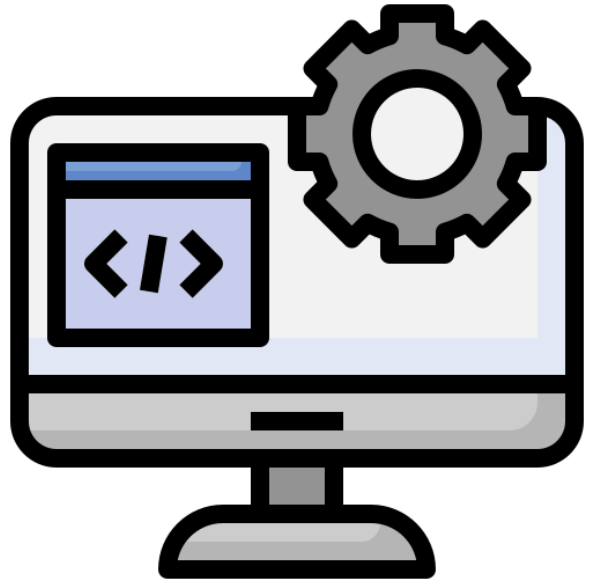


OUTILS DE SÉCURITÉ A UTILISER

- Garder ses outils a jour : système d'exploitation, antivirus, pare-feu
- Utiliser les outils mis a disposition : Utilisez un VPN si possible
- Limiter les permissions : Utiliser des sessions personnelles et limiter les droits des utilisateurs qui ne partageront pas leur mots de passe

OUTILS/ LOGICIELS A NE PAS UTILISER

- Logiciels de source non officielle : les logiciels qui ne proviennent pas du site officiel constituent une menace pour la machine et pour le réseau
- Moyens de communication non sécurisés : il y’a des risques de phishing présents et si les données ne sont pas chiffrées elles peuvent fuiter
- VPN autre que celui mis à disposition par l’entreprise : ils peuvent ne pas être conformes avec les principes de sécurités mis en place



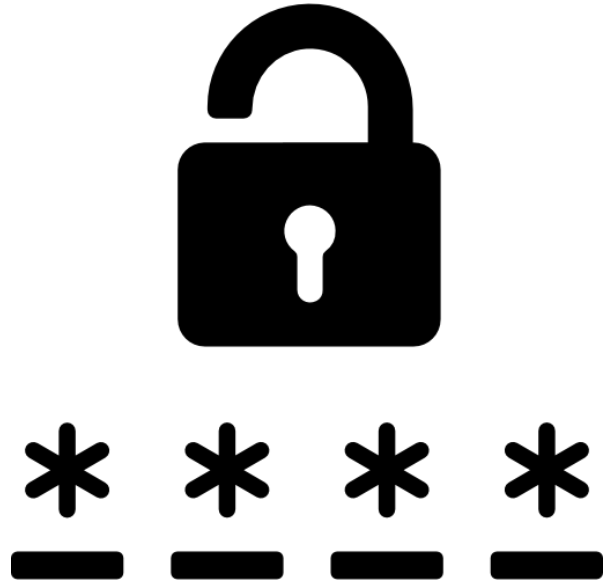
OUTILS DE COMMUNICATION

- Vérifier les conditions d'utilisation avant d'utiliser un service
- Utiliser des outils de communication chiffrés : Tixeo recommandé par l'ANSSI
- Chiffrer les données avant de les transmettre et transmettre lemot de passe par SMS , les données peuvent être chiffrées avec <<7-Zip

SÉCURITÉ DES MOTS DE PASSE

Un mot de passe doit être :

- Long
- Complexe
- Different pour chaque service/équipement
- Activer la double authentication



SENSIBILISATION

- Prévenir les utilisateurs des risques
- Mettre en place une charte qu’ils devront accepter et respecter sous peine de sanctions

DIFFERENCES PRATIQUES PERSONNELLES ET PROFESSIONELLES

Différencier pratiques professionelles/personnelles :

La responsabilité est différente d'un point de vu personnel et professionnel, l'entreprise peut avoir à manipuler des données de personnes et donc avoir une grande responsabilité et de manière générale les utilisateurs dans le domaine personnel sont peu prudents (mot de passes, services non sécurisés utilisés, messageries utilisées etc...) il est donc essentiel d'être prudent du point de vue professionnel et d'utiliser des services différents du domaine personnels s'ils ne sont pas sécurisés