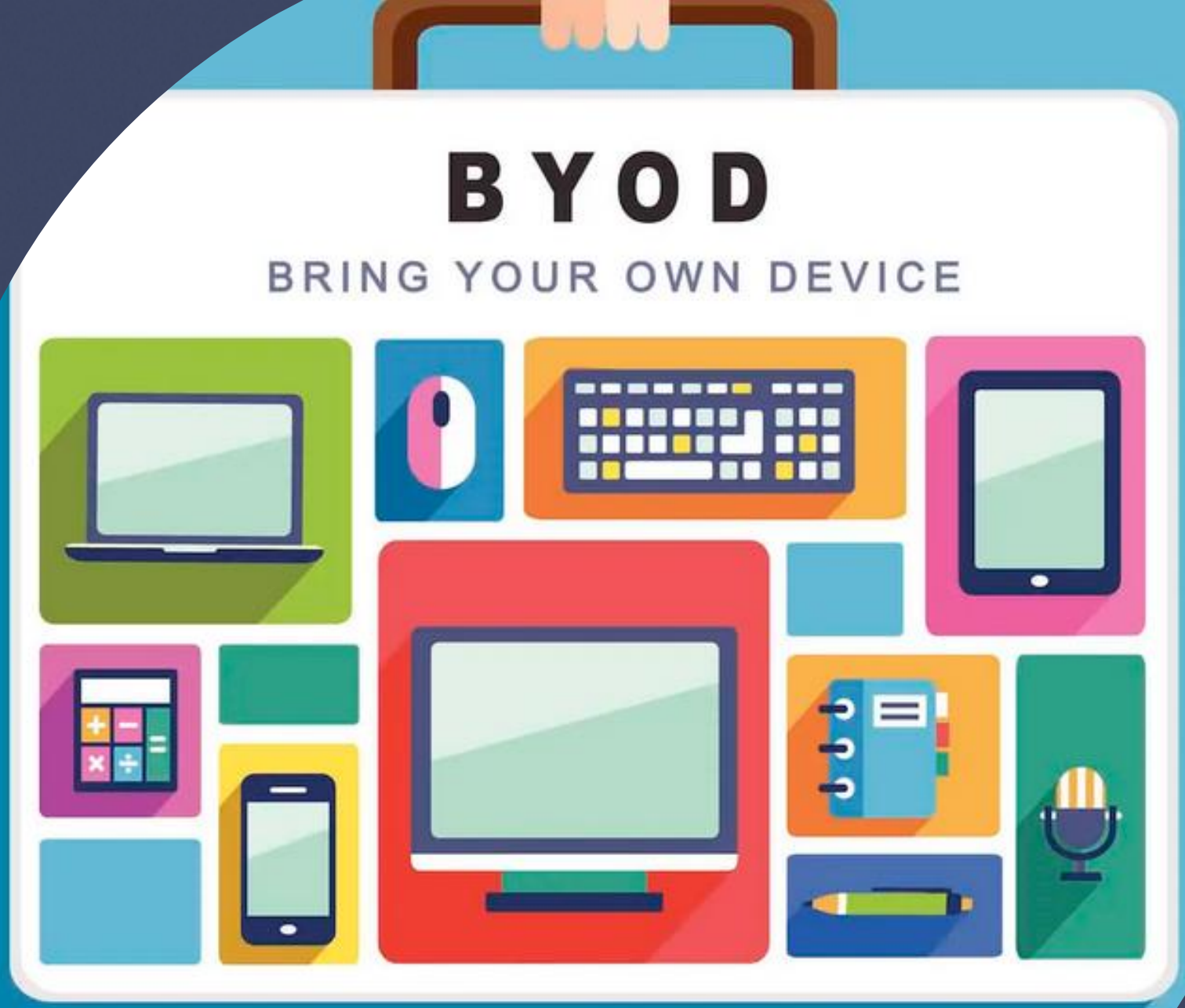
TP 2 – Mise en place des bonnes pratiques



Qu'est-ce que le BYOD ?

BYOD, qui est l'abréviation de "Bring Your Own Device", désigne l'usage d'un équipement informatique personnel dans un contexte professionnel.

Par exemple, un collaborateur se connecte au réseau de l'entreprise avec un ordinateur portable personnel.

Si l'on souhaite en bénéficier, il faudra alors faire une mise en balance des intérêts et des inconvénients pour l'usage d'un équipement qui fera la frontière entre vie personnelle et professionnelle.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

1. Liste d'outils utilisables pour sécuriser un poste informatique

- Vpn (Cisco AnyConnect, OpenVPN)
- Gestionnaire de mot de passe (LockPass)
- Un antivirus (Windows Defender, Avast, BitDefender)
- Un anti-spam (Mailinblack)
- Un pare-feu (Celui de Windows, Cisco ASA pour les grandes infrastructures réseaux, SonicWall pour les plus petites/moyennes entreprises)
- Mise à jour (Windows Update, des logiciels applicatifs...)
- Limiter les droits d'utilisateurs en fonction des besoins
- Offrir des solutions de stockage de donnée par cloud
- Télécharger des fichiers (uniquement sur une liste blanche prédéfinit)
- Effectuer des sauvegardes du système régulièrement (utile en cas d'attaque d'hameçonnage)

https://www.cnil.fr/fr/securite-securiser-les-postes-de-travail

2. Liste d'outils/logiciels qui ne peuvent être présents sur un poste informatique

Il est important pour préserver l'environnement de travail des possibles indésirables de le protéger en évitant certains outils/logiciels pouvant atteindre l'intégrité de l'entreprise.

- Logiciels de partage non sécurisés (µTorrent, BitTorrent, eMule...)
- Logiciels de piratage (WireShark, John the Ripper...)
- Logiciels de communication non autorisé (Telegram, Wechat...)
- Outils de virtualisations (peut contourner la sécurité de l'entreprise)
- Outils permettant de contourner la sécurité des pare-feux (Tor)
- Outils de divertissement (Netflix, Steam)
- Outils de partage réseau (FileZilla, Nmap, Putty)
- Bloqueur de publicité non autorisé (AdBlock, uBlock)

3. Liste d'outils de communication

Microsoft Teams : permet d'avoir une messagerie, de faire des appels audio/vidéo, de SharePoint un outil de collaboration sur des documents partagés

Trello permet d'organiser ses projets avec un système de tableaux et d'assignations de tâches (vous pouvez insérer des images, des pièces-jointes, ajouter des membres en fonction de la tâche à accomplir...)

Microsoft OneDrive : permet de partager ses fichiers sur un cloud, stockage sécurisé avec sauvegarde et gestion de droits/permissions pour la confidentialité

Pour les courriels, Microsoft Outlook ou bien Gmail sont deux solutions complètes et fiables (chiffrement et protection contre les spam)

4. La politique de sécurité des mots de passes pour les postes informatiques

- Le mot de passe par défaut doit être changé
- Un mot de passe long (au moins 12 caractères)
- Complexité (Majuscules, chiffres, caractères spéciaux)
- Changer son mot de passe régulièrement (tous les 3 mois)
- Verrouillage du compte après plusieurs tentatives échoués
- Sensibilisation régulière sur les bonnes pratiques
- Utiliser un gestionnaire de mot de passe

5. Sensibilisation au pratique du BYOD

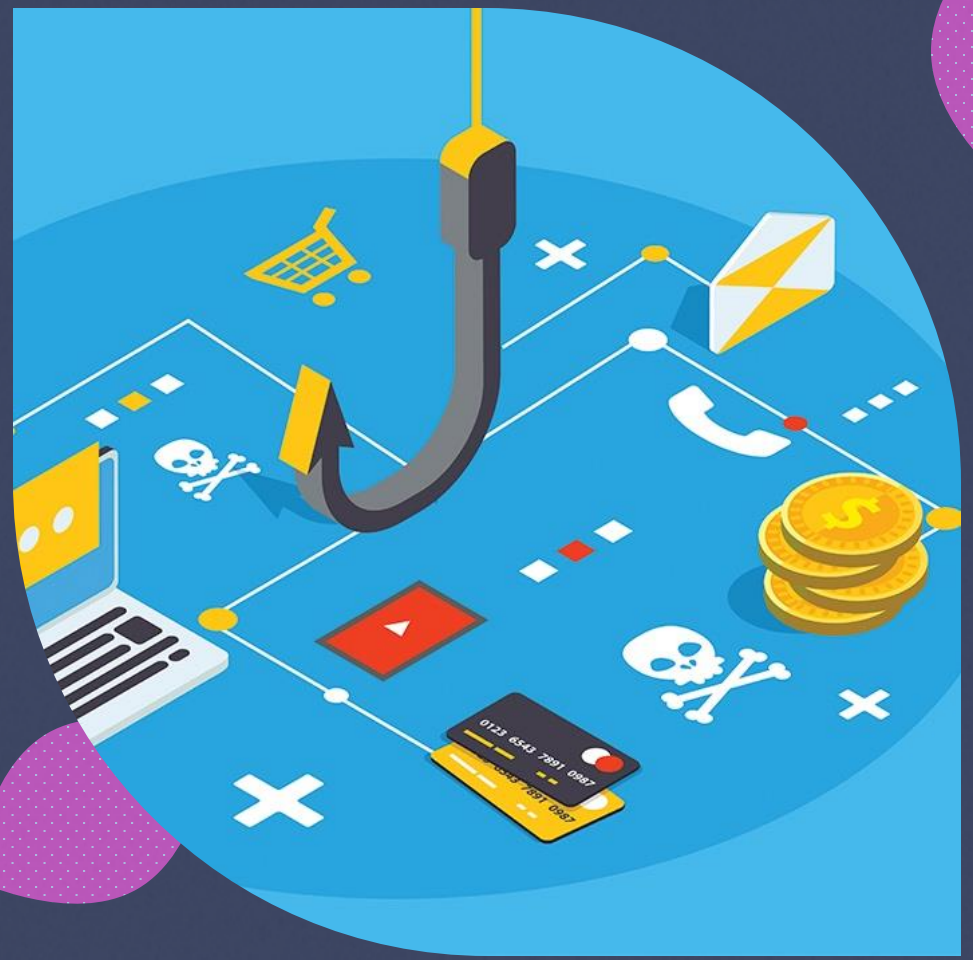
3 risques à anticiper : l'impossibilité pour le salarié d'accéder aux ressources qu'il a besoin, la contamination du système (faille de sécurité) et la fuite/perte de données

Nous allons instaurer:

- **Une charte informatique** (pour recenser les bonnes pratiques)
- **Des sessions d'e-learning** (former des collaborateurs selon leur rythme)
- **Des formations de groupe**
- **Des dispositifs ludiques et participatifs** (mise en place de quiz, des mises en situations vidéo...)

Pour se faire quelques règles seront nécessaires :

- **Être encouragé par la direction**
- **Proposer des contenus pratiques liés aux usages réels des utilisateurs**
- **Se limiter à quelques sujets importants, dans le contexte de l'entreprise.**
- **Mené ces formations à des équipes complètes et pas certains collaborateurs**
- **Offrir des rappels réguliers suivant l'évolution des menaces**



https://www.stormshield.com/fr/actus/lhumain-cle-de-la-cybersecurite-des-entreprises/

6. Synthèse sur les bonnes pratiques personnels et professionnels

Les bonnes pratiques personnels et professionnels :

- **Utiliser des mots de passe** différents en fonction des services professionnels et personnels que vous accédez
- **Ne pas mélanger sa messagerie professionnelle et personnelle** (se faire pirater son compte personnel mettrait en danger l'entreprise)
- Une utilisation saine d'internet au travail (éviter les sites de téléchargement illégaux, des contenus avec droit d'auteur, des propos condamnables et d'autres encore...)
- **Ne pas mélanger les services de stockage en ligne** du point de vue personnel et professionnelle (du moins si vous n'avez pas mis de mesure de sécurité au préalable)
- **Faire les mises à jour de sécurité** de vos équipements
- **Mettre en place des antivirus** contre les attaques potentielles
- Installer des applications uniquement depuis des sites officiels
- **Se méfier des périphériques** (USB, disque dur...)
- **Éviter les réseaux non reconnus** (certains sont contrôlé par des cybercriminels qui peuvent récupérer vos informations personnelles)

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso