



# LES BONNES PRATIQUES POUR LA SÉCURITÉ INFORMATIQUE

**Sensibilisation** aux bonnes pratiques de la **sécurité informatique** (cybersécurité), afin de **limiter les risques** de cyberattaque, piratages informatiques liés à internet.

# BONNES PRATIQUES À CONNAÎTRE



## Mots de passe

- » Entre 9 et 16 caractères  
Recommandation de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
- » De préférence, utilisez une **“pass phrase”** contenant des caractères spéciaux, avec des chiffres et des majuscules dans le corps de la phrase, ni au début, ni à la fin

Exemple : *lemoutonBleu?m@nge*

- » Ne pas préenregistrer ses mots de passe
- » Utiliser un gestionnaire de mot de passe agréé par la Cyber Team (ex : KeepassXC)



## Déplacements pro

- » **INTERDIT** : Utilisation des wifi gratuit à l'hôtel, dans les avions, aéroports,...
- » Se déplacer uniquement avec les derniers fichiers utiles à la mission
- » Sauvegarder ses données
- » Garder sur soi les appareils, supports et fichiers
- » Refuser la connexion d'équipements d'une tierce personne sur vos appareils



## Clefs USB



- » **ATTENTION** : Ne pas utiliser de clefs USB trouvées !

# CYBERATTAQUE

## LIMITER LES RISQUES

### Antivirus



- » Redémarrer les ordinateurs une fois par semaine afin d'installer les mises à jour nécessaires
- » Lancer des scans antivirus approfondis une fois par mois (pour savoir comment faire contactez Nicolas BONNET)



### Gestion des PC

- » Verrouiller son ordinateur lorsque l'on quitte son poste de travail avec les touches Windows + L
- » Éteindre régulièrement les ordinateurs (vacances, week-end,...)



### Séparer l'usage professionnel & personnel

- » Créer des mots de passe différents entre les services
- » Ne pas utiliser un stockage pro à des fins personnelles et inversement



### Gestion des e-mails

- » Vérifier la légitimité de l'émetteur (logo, format,...)
- » Ne pas ouvrir de pièces jointes ou de liens sans connaître l'expéditeur
- » Sauvegarder les mails importants sur les serveurs (rapprochez-vous de la Cyber Team pour connaître la marche à suivre)



### Sauvegarde

- » Evitez de sauvegarder sur le poste de travail, FAVORISER les sauvegardes sur le réseau (en cas de perte, de vol,... les fichiers SUR le poste seront PERDUS !)





# CYBERATTAQUE

## TROUSSE DE 1ER SECOURS

### 01/ DÉBRANCHEZ TOUT



- » Eteindre tous les postes, les serveurs, les switchs... même de façon brutale
- » **Objectif** : Couper tous les accès externes aux équipements
- » Stopper l'ouverture de tous les mails en provenance de la société attaquée
- » Stopper toute tentative de connexion VPN

### 02/ INFORMEZ



- » Vos équipes afin qu'elles se déconnectent de tout accès
- » Votre prestataire informatique
- » Notre assureur :

Tél : 06.44.60.70.30

N° contrat : rd 01495186



### 03/ ALERTEZ VOTRE DIRECTION & LA CYBER TEAM :



**Nicolas PEILLON** : 06.33.68.87.05

**Nicolas BONNET** : 06.50.42.31.69

**Damien DELOBEL** : 06.63.17.88.71

