Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'AGRICULTURE
DE L'AGROALIMENTAIRE
ET DE LA FORÊT

GUIDE DES BONNES PRATIQUES DE L'INFORMATIQUE

10 règles pour sécuriser les équipements numériques professionnels

MISSION DÉFENSE / MSSI

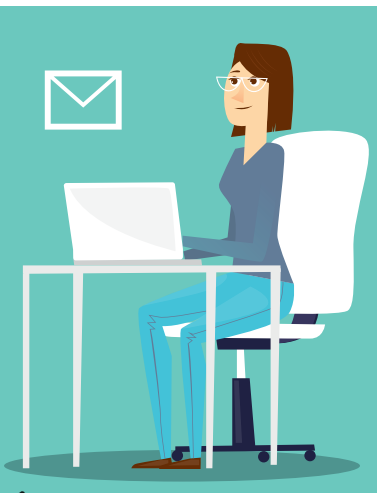
01 LE MOT DE PASSE

~~motdepasse~~ ~~minagri~~ ~~1234~~

Le mot de passe doit être personnel, ni partagé, ni affiché.

Un bon mot de passe comprend au moins 8 caractères et inclut :
- des majuscules,
- des minuscules,
- des chiffres,
- des caractères spéciaux.

02 LA MESSAGERIE



Ne pas ouvrir les **messages ou pièces jointes suspects** et avertir l'informatique de proximité dès leur réception.

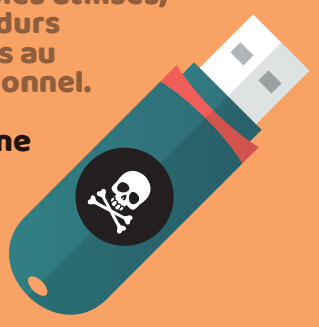
Ne pas cliquer sur des **liens internet suspects** ou qui demandent un login et mot de passe.

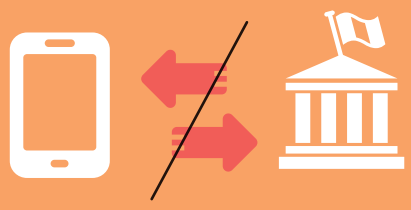
~~Hotmail~~ ~~YAHOO!~~ ~~Gmail~~

Ne jamais transférer la messagerie professionnelle sur une messagerie personnelle.

03 SUPPORTS AMOVIBLES

Les supports amovibles utilisés, clés USB ou disques durs externes, sont dédiés au strict usage professionnel.
Ne jamais connecter une clé USB dont on ne connait pas l'origine sur du matériel professionnel.





Il est interdit de connecter du matériel personnel sur le réseau du ministère : ordinateur portable, smartphone, tablette...

04 MATÉRIEL PERSONNEL

05 INSTALLATION DE LOGICIELS

Ne pas télécharger ni installer de logiciels qui ne soit pas autorisé par l'informatique de proximité.

06 AU BUREAU

Ne pas laisser de documents sensibles sur le bureau, à l'imprimante, en salle de réunion...

Ces documents sont rangés dans un meuble fermant à clé.

Activer le vérouillage automatique de l'ordinateur, tablette, smartphone...

07 SITES, BLOGS, FORUMS, RÉSEAUX SOCIAUX

Ne pas utiliser l'adresse mail ni le mot de passe professionnels pour s'inscrire sur une plate-forme extérieure au réseau du ministère.

Ne pas partager des informations professionnelles sur les **réseaux sociaux,** ni porter atteinte au ministère.

08 CHIFFREMENT

En déplacement, pour éviter le vol de données, **utiliser des ordinateurs portables ou des tablettes dont les données sont chiffrées.**

09 MOBILITÉ

Ne pas laisser son matériel portatif sans surveillance. À l'étranger, le garder avec soi.

Ne pas connecter d'appareils à des réseaux Wifi, Bluetooth ou NFC publics : gares, aéroports, hôtels, transports, salle de réunion extérieures... Désactiver ces modes de communication s'ils ne sont pas utilisés.

Au retour d'une mission à l'étranger, **faire expertiser son matériel** par l'équipe informatique.

10 INCIDENTS & ALERTES

Ne pas ignorer un incident sur du matériel professionnel, **donner l'alerte rapidement auprès de l'équipe de l'informatique de proximité** afin que les mesures adéquates soient prises.