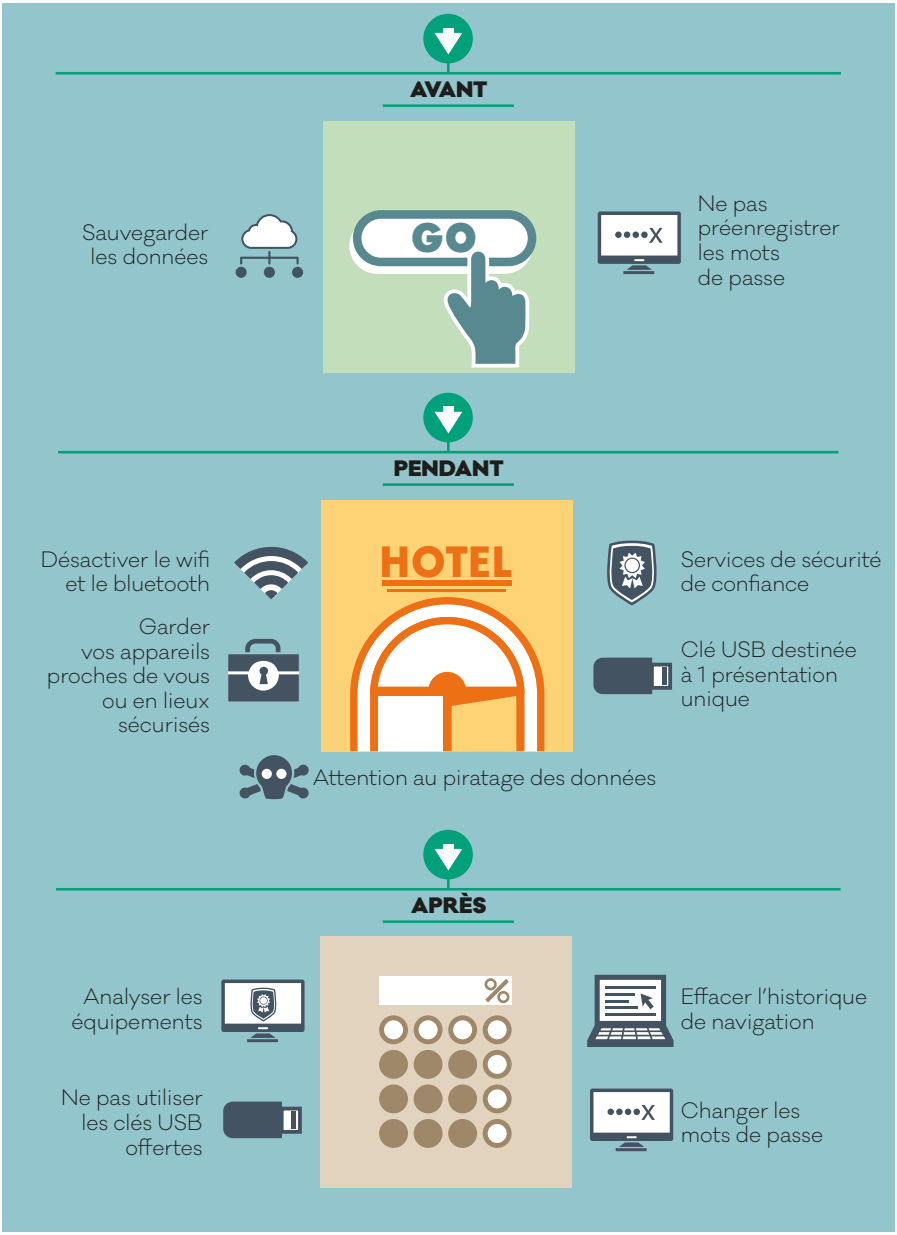
LES RÈGLES DE SÉCURITÉ LORS DU DÉPLACEMENT PROFESSIONNEL



Par-delà ces bonnes pratiques, il est possible d'aller plus loin et de **bâtir une politique de sécurité globale** qui prenne en compte toutes les étapes du cycle de vie de la donnée (acquisition, création, communication, stockage, mise à jour, destruction).

Cette politique de sécurité couvrira des aspects variés, tels que :
- nomination d'un responsable sécurité et identification des responsabilités dans l'entreprise ;
- classification des informations en fonction de leur degré de sensibilité (rares, vulnérables, stratégiques) ;
- définition des règles d'accès (bâtiments, informatiques, internet…) ;
- rédaction et diffusion de procédures de sécurité quotidiennes ;
- communication des mesures spécifiques aux données à adopter en cas d'incendie ;
- rédaction et diffusion d'une charte précisant les usages autorisés des équipements informatiques mis à la disposition des collaborateurs ;
- définition d'un plan de continuité d'activité…

LES PRATIQUES EN ENTREPRISES

La sécurité des données est prise très au sérieux par les grandes et moyennes entreprises. Pour les PME, cela recouvre des réalités très variées, souvent complexes et imbriquées.

Il est clair qu'en l'espèce, **il n'existe pas de risque zéro** : tout l'enjeu pour l'entreprise est donc de réduire les risques à un niveau acceptable sans pour autant entraver son bon fonctionnement.

Les entreprises les plus sensibles à la perte des données utilisent des méthodes draconiennes pour se protéger. L'usage d'Internet est limité à quelques postes fixes connectés à un réseau différent du reste de l'entreprise.
En déplacement, un ordinateur sans donnée et une clef *USB* chiffrée sont mis à disposition du collaborateur (l'accès aux fichiers se fait par des serveurs distants sécurisés).
Le voyageur n'a pas de smartphone mais un téléphone d'entreprise basique.

Afin d'accompagner les entreprises dans la gestion de leur sécurité informatique, l'état français, via l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) propose un *MOOC* - *SecNumacadémie* - dont l'objectif est de permettre à tous d'être initiés à la cyber sécurité ou d'approfondir leurs connaissances afin de pouvoir agir efficacement sur la sécurité de leurs systèmes d'information (SSI) au quotidien.

POINTS D'ATTENTION

- Définir une stratégie
- Engager la direction de l'entreprise
- Sensibiliser les salariés aux pratiques responsables

CHANGEMENTS ET IMPLICATIONS

La gestion de **la protection des données risque d'être complexifiée par les comportements des collaborateurs**. De plus en plus mobiles, les voyageurs aiment à se retrouver dans des lieux de travail atypiques (café, espaces de *co-working*…).
Il est alors encore plus important de les sensibiliser aux risques encourus.

CONTRAINTES

Il est important de trouver le juste équilibre entre protection de l'entreprise et mise à profit des nouvelles technologies.

CONSEILS PRATIQUES

- Procédez à des **mises à jour régulières** de vos logiciels.
- Soyez **prudents lors de vos achats en ligne**, privilégiez les sites sécurisés (*https* et présence d'un cadenas dans l'affichage de votre navigateur).
- Gérez et **organisez l'accueil de vos visiteurs** (badges, parcours construits de manière à ce qu'ils ne voient pas les équipements et documents…).
- **Sensibilisez votre personnel** en déplacement (ne pas travailler sur des documents sensibles / confidentiels ni avoir de discussions professionnelles dans les lieux publics en citant les noms et sociétés de vos correspondants / clients / collaborateurs / fournisseurs).
- Soyez aussi **prudent avec votre *smartphone*** / tablette qu'avec votre ordinateur.
- **Séparez les usages personnels et professionnels**.
- **Réservez un PC portable pour les déplacements** (avec un minimum d'informations et une sacoche discrète, différente de celle d'origine du constructeur).
- Mettez à disposition des collaborateurs **des filtres de confidentialité** à poser sur les écrans des PC.
- **Stockez au maximum vos données sur des serveurs distants** plutôt que sur le PC (en cas de vol / espionnage, aucune donnée confidentielle n'est ainsi disponible immédiatement).
- **Utilisez des mots de passe différents** pour chaque application et ne les stockez pas sur l'ordinateur (ou sur un papier laissé dans la pochette).