



## **REGLES DE SECURITE DANS L'ERE DU DIGITAL**

**Les bons réflexes à avoir ...**

**...« Priorité à la confidentialité »**

### **Sur INTERNET**

- Soyez vigilant lors de la consultation de sites sensibles
- Veillez à être connecté à un réseau de confiance et en cas de paiement vérifiez que le site est sécurisé : https://
- Soyez discrets : consulter à l'abris des regards et utilisez un filtre écran de confidentialité

### **Sur votre MESSAGERIE**

- N'ouvrez pas les pièces jointes de messages de provenance inconnue ou douteuse
- Veillez à la syntaxe, à la grammaire et l'orthographe des messages reçus : phishing...
- Refusez de communiquer des données sensibles : numéro de carte, login, mot de passe...
- En présence d'un lien hypertexte demandez-vous :  
    Vers quelle adresse pointe ce lien ? L'action demandée est-elle licite ?
- Contactez directement la personne pour lever le doute !

### **Sur les SYSTEMES D'INFORMATION**

- Pour traiter des informations sensibles évitez de vous connecter à des réseaux WIFI publiques (gare, hôtel, restaurant...)
- Privilégiez l'usage d'un VPN pour sécuriser vos échanges
- Ne branchez pas sur votre système d'information de clés USB ou d'objets connectés d'origine inconnue
- Privilégiez de recharger votre téléphone sur une prise secteur plutôt que sur votre système d'information
- Veillez à mettre à jour votre système d'exploitation, votre antivirus , vos applications...

### **Sur vos MOTS DE PASSE**

- Ils doivent comporter 12 caractères au minimum, des majuscules, minuscules, des chiffres et caractères spéciaux
- Ils doivent être non signifiants, ne pas avoir de lien direct avec vous (dates, lieu de naissance...), il est possible de retenir les 1eres lettres des mots d'une phrase : Des arbres trois fois trop lourds : D@3ftl

- Le mot de passe ne doit idéalement servir que pour un seul accès /compte et ne doit pas être réutilisé ailleurs
- Vous pouvez : utilisez un coffre-fort numérique pour stocker vos différents mot de passe (site de l'ANSSI)

***Quelques outils pour vous protéger :***

*USB port blocker : outil permettant de bloquer physiquement les ports USB de vos ordinateurs pour en contrôler l'accès.*

*USB Data Filter : outil permettant de recharger votre téléphone ou tout autre objet connecté en inhibant la liaison de données.*

**Pour toute information contacter la DGSi : [groupeasd@interieur.gouv.fr](mailto:groupeasd@interieur.gouv.fr)**