Le RGPD : Alors, que faire ?

Le choses à éviter :

- Pour les mails : vérifier l'émetteur, l'objet, les pièces jointes; ne pas ouvrir trop vite !

Ce qui vous alerte : fautes d'orthographe, offres promo, tirage au sort, un ami dans le besoin, un lien internet étrange, la présence d'une pièce jointe

- Comprendre que tous les équipements connectables en USB contiennent de l'intelligence.

Les bonnes pratiques :

- Je regarde et j'analyse avant de cliquer
- Je mets les mails suspects à la poubelle
- Je ne transfère pas d'infos sensibles par mail
- Je n'ouvre pas les pièces jointes suspectes
- Je ne connecte pas de support USB inconnu
- Je contrôle les périphériques USB que je dois connecter
- J'utilise Nuage ou OneDrive pour le transfert de documents ou d'infos sensibles.

Votre identifiant et votre mot de passe sont personnels et confidentiels et ne doivent JAMAIS être communiqués :

Mot de passe :

- je le change tous les 120j
- je choisi un mot de passe qui n'a pas de lien avec moi ; environ 12 caractères de types différents
- je ne stocke pas les mots de passe dans un endroit facile d'accès (fichier, post-it..)
- je ne demande pas à un tiers de faire MON mot de passe
- je n'enregistre pas mes mots de passe sur le navigateur web

Gestion des mots de passe :

- je choisi des mots de passe complexes que je change régulièrement
- je privilégie la double authentification quand c'est possible
- j'utilise un Gestionnaire de mots de passe : KeePass, Bitwarden ….
-

Les règles pour l'ordinateur de travail :

- je ne partage pas mon ordi avec la famille s'il s'agit de mon outil de travail
- je n'installe pas de logiciels non autorisés
- je ne vais pas sur des sites à risques
- je tiens mon équipement à jour

- je mets un mot de passe pour l'ouverture de mon ordi
- je mets un mot de passe sur le logiciel métier
- j'utilise un antivirus, Firewall, Proxy…
- je protèges mes emails Proofpoint
- je passe à Office 365
- je demander à mon informaticien de chiffrer le disque dur (ce qui veut dire qu'il faudra un code à rallonge pour le décrypter)
- j'ai un hébergeur de données en France ou en Europe.

Tout ceci est également valable pour la vie privée !!

NI