Principes généraux d'hygiène numérique et de sécurité

La sécurité complète à 100% n'existe pas, mais il y a des moyens de réduire les risques

La FMH a édicté plusieurs recommandations de bonnes pratiques au sujet de la sécurité informatique que vous pouvez trouver:sur leur site ici

- S'assurer d'avoir une **sauvegarde interne séparée** de son serveur ainsi qu'une **sauvegarde externe (géographiquement)**. Ces sauvegardes doivent être régulières (nombre de minutes/heures que vous êtes prêts à perdre), fonctionnelles (à vérifier), **cryptées** et comprendre toutes les données que vous n'acceptez pas de perdre !
- **Antivirus/pare-feu** à jour y compris sur les systèmes équipés de Mac OS
- Faire régulièrement les **mises à jour** système et des programmes internes du matériel (p.ex. routeur)
- Utiliser des **mots de passe complexes et uniques** (via un gestionnaire de mot de passe p. ex) et activer l'authentification par deux facteurs lorsque cela est possible
- **Chiffrer ses disques durs** (fonction en principe dorénavant incluse directement dans les systèmes, voir avec son informaticien)
- **Ne pas cliquer sur des liens suspects** envoyés par mail (informer les secrétaires et assistantes médicales, faire signer une charte de bonne conduite)
- Considérer **éteindre son serveur et/ou sa connexion internet** durant les périodes d'inactivité p.ex. la nuit, vacances (cave : en concertation avec votre informaticien !)
- **Supprimer les données dont on a plus besoin** et dont on a pas l'obligation légale de les conserver (p.ex une fois que les documents ont été insérés dans le logiciel primaire) selon le principe “Les données que nous n'avons pas/plus ne peuvent pas nous être volées !”
- Avoir un **plan de crise** en cas d'attaque
- Considérer **s'assurer contre le risque de cybersécurité** (frais de restauration, perte d'exploitation, préjudice à des tiers...)