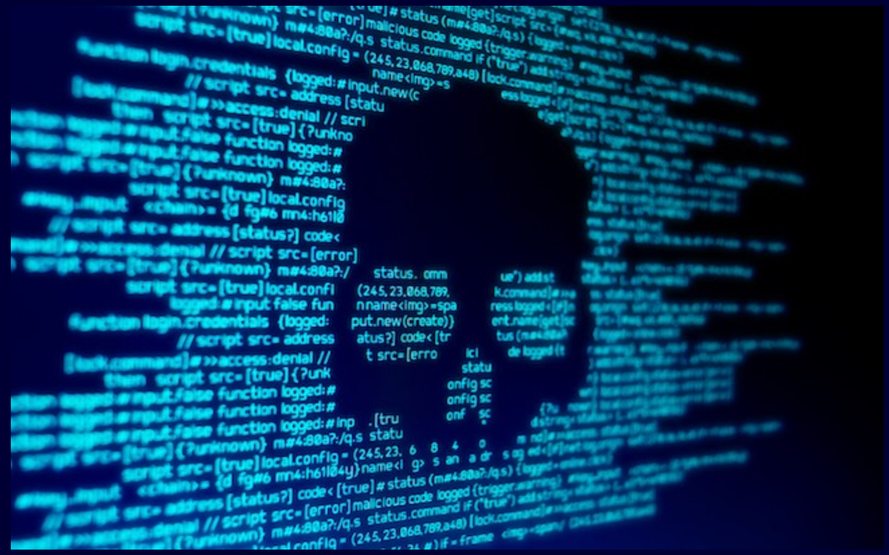
Bonnes pratiques



La sécurité informatique

De quoi s’agit-il ?

- Sécurité des données
  - Contre les pertes « physiques »
  - Contre les pertes « logicielles »
- Sécurité des utilisateurs
  - Accès aux données
  - Préservation de la vie privée

Sécurité des données

Contre les pertes physiques :

- Panne matérielle (typiquement disque dur)
- Incendie
- Surtension électrique (foudre)
- Dégât des eaux
- Vol, cambriolage

… comment s’en prémunir ?

- Trois réponses :
  - Sauvegarde
  - Sauvegarde
  - Sauvegarde
- Varier les supports (disque externe, NAS, cloud, carte mémoire, second ordi synchronisé…)
- Automatiser la création de sauvegarde
- Séparer physiquement la sauvegarde de l’ordinateur principal
- Avoir au moins une sauvegarde non synchronisée (ie. pas un cloud : synchro des virus)

Sécurité des données

Contre les pertes logicielles :

- Plantage, bug logiciel
- Fausse manip, effacement accidentel
- Virus
- Ransomware
- Malware

… comment s’en prémunir ?

- Maintenir son système et tous ses logiciels à jour
- Utiliser un antivirus, mis-à-jour automatiquement
- Activer les différents dispositifs de sécurité de son système (firewall en particulier)
- Ne pas utiliser son ordinateur en tant qu’administrateur
- Être très attentif aux liens et pièces jointes de ses e-mails (voire un peu parano)
- Disposer d’une sauvegarde fréquente, mais pas synchronisée en temps réel (attention au cloud)

Faire un audit de ses données

- Celles que l’on peut remplacer immédiatement (système, logiciels, …)
- Celles que l’on accepte de perdre sans regret (téléchargements, PJ de mails conservés ailleurs)
- Celles que l’on peut retrouver facilement (musique achetée en ligne)
- Celles qui représentent beaucoup de travail (documents professionnels)
- Les données irremplaçables (photos, archives)

- Adopter une politique différenciée pour la sauvegarde des données

Sécurité des utilisateurs

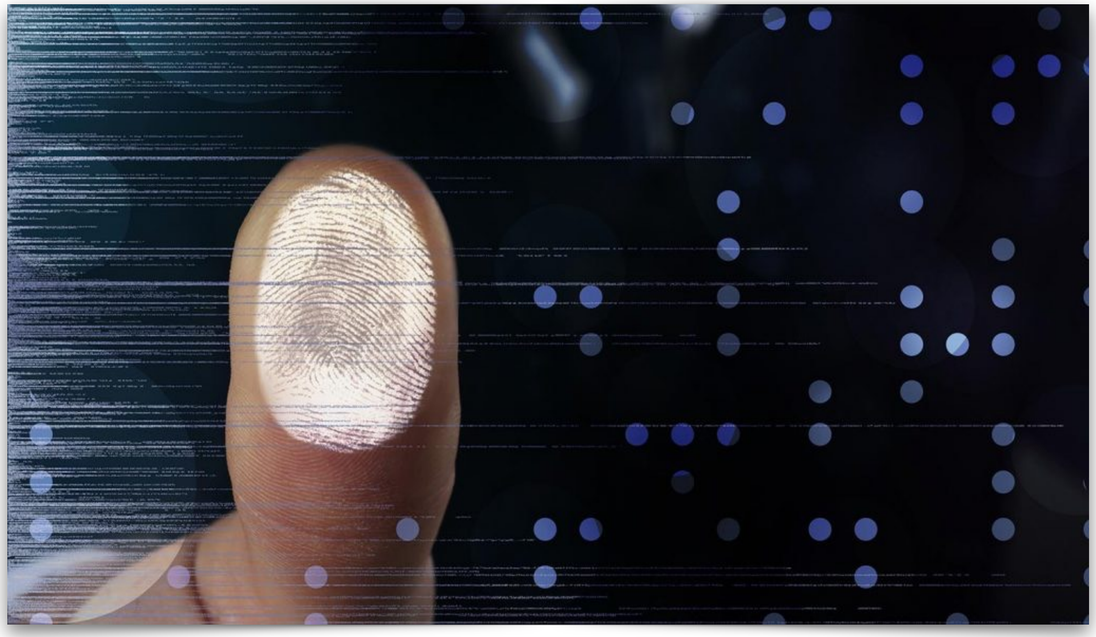
Concernant l'accès aux données

- Mots de passe robustes et différents sur chaque compte !
- Adopter une politique de mot de passe / utiliser un coffre fort (Keepass)
- Etre très attentif à la sécurité de sa boite mail principale
- Cryptage du disque dur
- Conteneur crypté (VeraCrypt)
- Utiliser la double authentification dès qu'elle est disponible

Sécurité des utilisateurs

Concernant la vie privée

- Être attentif à son identité en ligne
- Utilisation des réseaux sociaux : paramétrer correctement les paramètres de partage
- Utiliser un pseudonyme lorsque c’est possible
- Être attentif aux traces que l’on laisse (cookies, flash…)
- Empreinte ou fingerprint (voir navigateur Brave)
- VPN
- Paramétrage des logiciels et appareils



10 commandements de l'ANSSI

- Utiliser des mots de passe de qualité
- Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel...
- Effectuer des sauvegardes régulières
- Désactiver par défaut les composants ActiveX et JavaScript
- Ne pas cliquer trop vite sur des liens
- Ne jamais utiliser un compte administrateur pour naviguer
- Contrôler la diffusion d'informations personnelles
- Ne jamais relayer des canulars
- Soyez prudent : l'internet est une rue peuplée d'inconnus !
- Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants